

THE FUTURE OF MONEY—PART 2

Y 4. B 22/1: 104-27/PT. 2

The Future of Money-Part 2, Serial...

HEARING

BEFORE THE

SUBCOMMITTEE ON

DOMESTIC AND INTERNATIONAL MONETARY POLICY

OF THE

COMMITTEE ON BANKING AND

FINANCIAL SERVICES

HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTH CONGRESS

FIRST SESSION

OCTOBER 11, 1995

Printed for the use of the Committee on Banking and Financial Services

Serial No. 104-27

U.S. GOVERNMENT PRINTING OFFICE
DEPOSITORY



MAR 28 1996

U.S. GOVERNMENT PRINTING OFFICE

20-128 CC

WASHINGTON : 1996

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402

ISBN 0-16-052240-4

THE FUTURE OF MONEY—PART 2

Y 4. B 22/1:104-27/PT. 2

The Future of Money-Part 2, Serial...

HEARING

BEFORE THE
SUBCOMMITTEE ON
DOMESTIC AND INTERNATIONAL MONETARY POLICY
OF THE
COMMITTEE ON BANKING AND
FINANCIAL SERVICES
HOUSE OF REPRESENTATIVES
ONE HUNDRED FOURTH CONGRESS

FIRST SESSION

OCTOBER 11, 1995

Printed for the use of the Committee on Banking and Financial Services

Serial No. 104-27



MAR 28 1996

U.S. GOVERNMENT PRINTING OFFICE

20-128 CC

WASHINGTON : 1996

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-052240-4

HOUSE COMMITTEE ON BANKING AND FINANCIAL SERVICES

JAMES A. LEACH, Iowa, *Chairman*
BILL MCCOLLUM, Florida, *Vice Chairman*

MARGE ROUKEMA, New Jersey	HENRY B. GONZALEZ, Texas
DOUG BEREUTER, Nebraska	JOHN J. LAFALCE, New York
TOBY ROTH, Wisconsin	BRUCE F. VENTO, Minnesota
RICHARD H. BAKER, Louisiana	CHARLES E. SCHUMER, New York
RICK LAZIO, New York	BARNEY FRANK, Massachusetts
SPENCER BACHUS, Alabama	PAUL E. KANJORSKI, Pennsylvania
MICHAEL CASTLE, Delaware	JOSEPH P. KENNEDY II, Massachusetts
PETER KING, New York	FLOYD H. FLAKE, New York
EDWARD ROYCE, California	KWEISI MFUME, Maryland
FRANK D. LUCAS, Oklahoma	MAXINE WATERS, California
JERRY WELLER, Illinois	BILL ORTON, Utah
J.D. HAYWORTH, Arizona	CAROLYN B. MALONEY, New York
JACK METCALF, Washington	LUIS V. GUTIERREZ, Illinois
SONNY BONO, California	LUCILLE ROYBAL-ALLARD, California
ROBERT NEY, Ohio	THOMAS M. BARRETT, Wisconsin
ROBERT L. EHRlich, Maryland	NYDIA M. VELAZQUEZ, New York
BOB BARR, Georgia	ALBERT R. WYNN, Maryland
DICK CHRYSLER, Michigan	CLEO FIELDS, Louisiana
FRANK CREMEANS, Ohio	MELVIN WATT, North Carolina
JON FOX, Pennsylvania	MAURICE HINCHEY, New York
FREDERICK HEINEMAN, North Carolina	GARY ACKERMAN, New York
STEVE STOCKMAN, Texas	KEN BENTSEN, Texas
FRANK LOBIONDO, New Jersey	
J.C. WATTS, Oklahoma	BERNARD SANDERS, Vermont
SUE W. KELLY, New York	

SUBCOMMITTEE ON DOMESTIC AND INTERNATIONAL MONETARY POLICY

MICHAEL CASTLE, Delaware, *Chairman*
EDWARD ROYCE, California, *Vice Chairman*

FRANK LUCAS, Oklahoma	FLOYD H. FLAKE, New York
JACK METCALF, Washington	BARNEY FRANK, Massachusetts
BOB BARR, Georgia	JOSEPH P. KENNEDY II, Massachusetts
DICK CHRYSLER, Michigan	CAROLYN B. MALONEY, New York
FRANK LOBIONDO, New Jersey	LUCILLE ROYBAL-ALLARD, California
J.C. WATTS, Oklahoma	THOMAS M. BARRETT, Wisconsin
SUE W. KELLY, New York	CLEO FIELDS, Louisiana
ROBERT NEY, Ohio	MELVIN WATT, North Carolina
JON FOX, Pennsylvania	
	BERNARD SANDERS, Vermont

CONTENTS

	Page
Hearing held on:	
October 11, 1995	1
Appendix:	
October 11, 1995	41

WITNESSES

WEDNESDAY, OCTOBER 11, 1995

Blinder, Alan, Vice Chairman, Board of Governors of the Federal Reserve System	4
Crowell, William P., Deputy Director, National Security Agency	28
Diehl, Philip N., Director, U.S. Mint	31
Kammer, Raymond G., Deputy Director, National Institute of Standards and Technology	27
Katzen, Sally, Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget	15
Ludwig, Hon. Eugene A., Comptroller of the Currency	9
Morris, Stanley E., Director, Financial Crimes Enforcement Network	11
Rasor, Robert, Deputy Assistant Director for Investigation, Secret Service	32

APPENDIX

Prepared statements:	
Castle, Hon. Michael	42
Flake, Hon. Floyd H.	44
Blinder, Alan	60
Crowell, William P.	139
Diehl, Philip N.	146
Kammer, Raymond G.	131
Katzen, Sally	85
Ludwig, Hon. Eugene A.	48
Morris, Stanley E.	74
Rasor, Robert	160

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Diehl, Philip N., copy of Department of the Treasury's "National Performance Review—Phase II, Department of the Treasury—Final Proposals"	150
Kammer, Raymond G., biography	137
Katzen, Sally, Press Release from Executive Office of the President, dated June 14, 1995. "National Information Infrastructure Security Issues Forum Releases NII Security: The Federal Role"	94
Ludwig, Hon. Eugene A., written response to questions posed by Hon. Jack Metcalf	158

THE FUTURE OF MONEY—PART 2

WEDNESDAY, OCTOBER 11, 1995

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON DOMESTIC AND
INTERNATIONAL MONETARY POLICY,
COMMITTEE ON BANKING AND FINANCIAL SERVICES,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:19 a.m., in room 2128, Rayburn House Office Building, Hon. Michael N. Castle [chairman of the subcommittee] presiding.

Present: Chairman Castle, Representatives Metcalf, LoBiondo, Maloney, and Roybal-Allard.

Chairman CASTLE. The subcommittee will come to order.

Let me welcome everybody to the House Banking and Financial Services Committee, Subcommittee on Domestic and International Monetary Policy, which is the longest name of any committee, subcommittee in the House. And this is our second hearing on the future of money.

This subcommittee bravely continues to go where no one has gone before, although it is within the scope of our jurisdiction over important areas of public policy. The future of money, that is to say the shape and character of the future medium of exchange via electronic commerce, may well form the underpinning of the next expansion of worldwide commerce.

This intersection of technology and commerce has been predicted to fall on almost every point along a continuum ranging from overhyped fad to change with implications as profound as the industrial revolution. As we noted in our July hearing on the subject, whether it occurs over computers linked to the networks or via computer chips embedded in cards or other devices, the potential exists both for great commercial promise and for considerable risk of undermining currencies, systems of exchange, and the administration of justice.

It is incumbent upon Congress and the executive branch agencies, including law enforcement, to try to understand these technological innovations and the implications they hold for our future. For this reason, we have initiated this series of hearings.

It will not end with the session today. At least one more is in order. There I hope we can bring together representatives from banking, consumer groups, legal experts and technology companies not yet heard from.

The aim would be to initiate a process of consultation leading ultimately to private sector agreements that would address the key public policy questions that will be discussed today. I believe that

most of my colleagues on the subcommittee would share my preference to see Internet compacts and international industry agreements attempt to neutralize systemic threats. At least a genuine effort should be undertaken before turning to sovereign states to attempt the management of cyberspace.

You may be very certain that if this challenge is beyond the reach of the private sector, there will arise an irresistible pressure for government or some super-national authority to police this new world. This kind of official reaction can be expected only to stunt the development of commerce, arts, and other creative exchange across these electronic links.

The Financial Crimes Enforcement Network shares these concerns. They already have the responsibility of applying the Bank Secrecy Act in the countering of money laundering. They held a valuable cyberpayments colloquium 2 weeks ago in New York City, and the organization produced a useful working paper that is included in condensed form in each Member's folder.

We are pleased that Stan Morris, the FinCEN Director, has been able to make it back from China in time for the hearing today. At our last hearing we quoted Philip Diehl, the Director of the Mint, who will appear before the subcommittee today and tell us about the Mint's vision of electronic currency.

He has compared the current status of electronic forms of money to the situation before the Civil War, when local banks issued their own paper money. He foresaw that, left alone and unregulated, the market might produce an electronic Tower of Babel, with no technology standardization and many opportunities for law avoidance in criminal transactions. We are gathered to continue our exploration of these emerging third wave forms of currency and hear more about the appropriate role of the Federal Government.

This morning we will hear from eight expert witnesses drawn from the Federal Government. With their assistance, we can begin to consider some of these vital issues. For convenience, we have divided the group into two panels. The first has primary expertise to address aspects of the integrity of the monetary system, and the second will no doubt discuss issues of privacy, both commercial and personal. Both groups are free to overlap on issues and take the discussion where their particular institutional expertise leads them.

In short, we will consider in greater depth public policy issues raised at the first hearing. Cooperatives efforts between banks as an industry, and between banks and the government, have made current payment instruments successful and widely used. And if analogs to these precedents can be found for future payment mechanisms, they may be similarly successful.

We are fortunate to have before us eight eminent public servants who are charged with great responsibilities in the managing of our national economic security, law enforcement, sound money and communications security. They are Alan Blinder who is the Vice Chairman of the Board of Governors of the Federal Reserve System.

And missing for the time being because I shanghaied him for another meeting where he is right now, will be back in a moment, is Eugene A. Ludwig, who is the Comptroller of the Currency. Stanley

Morris is the Director of the Financial Crimes Enforcement Network. And Sally Katzen is the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, winning the title of the longest executive branch title.

Raymond Kammer is Deputy Director of the National Institute of Standards and Technology. William P. Crowell is the Deputy Director of the National Security Agency [NSA]. Philip Diehl is the Director of the U.S. Mint. And Robert Rasor the Deputy Assistant for Investigation of the Secret Service.

Obviously, the first four are the four we are going to hear from first, after we give the various Members an opportunity to make opening statements if they wish, we will turn to the witnesses and then have questions. And we will turn I guess correctly to Mrs. Maloney first, who has come in.

Mrs. MALONEY. Thank you, Mr. Chairman.

The time is not all that long ago that ATM machines first surfaced in our communities. I remember the questions about whether or not Americans would take favorably to electronic banking.

Mr. Chairman, we all now know they did. Americans sent a message, they put a premium on access to banking services that are designed to be available whenever, wherever and however it is most convenient. The products and services we will discuss today are the market's response to that strong message.

Exciting new technology has brought us smart cards, stored-value instruments, electronic currency and Internet transactions. Like the ATM, each of these offers new opportunities, opportunities for consumers and business, opportunities for more efficient flow of capital and commerce into this country, and indeed the world, opportunities that can be realized or missed, managed or mismanaged, properly regulated, underregulated, or overregulated. We need to be sure to strike the best balance and to make no rush to judgment.

At the consumer level, the greatest imaginable outcome is a vote where every American has a life of greater convenience, autonomy and safety because of these innovations, where parents can spend more time with their children and less time waiting in line at a bank or even an ATM, where seniors may have the option to receive social security or other benefits through a stored-value card, instead of having to redeem their benefits at a check-cashing stand, where some of our elderly are now the targets of muggers and thieves.

But there are also serious concerns; if we move away from the branch banking system, with more and more everyday transactions handled from home computers, will this affect the ability of the poor and underserved to access basic banking services? Or will the decreased transactional cost actually mean greater access where the home phone becomes a link to services currently unavailable in many communities?

I will certainly be watching the effect as these innovations are introduced. We all have a responsibility to watch this.

At the level of our national monetary policy we need to ask if and how stored-value balances may affect the way we measure and manage the money supply, and we need to be sure there is overall competitive equity between bank and nonbank issuers.

By calling these important hearings now, the chairman has anticipated these changes and given us the time for full and careful public discussion. That is how our legislative process works at its best, by anticipating, not just reacting.

And I thank the Chair for all his hard work.

Thank you.

Chairman CASTLE. Thank you, Mrs. Maloney.

Actually, something you said reminded me of something I think it is important to state here, and that is that these hearings are not the usual hearings that are—that predict legislation following. We are truly trying to find out in what direction we should go, and I have no suggestion of legislation, I don't think any of the Members do at this point. But we do feel that this is an area in which we need to define exactly what the future may hold.

We realize it is going to change very rapidly and a year from now we could have very different hearings. But I would just hasten to add that we are not preparing legislation; hopefully, you are not preparing regulations we don't know about at this time, but I think we need to communicate with each other about what could be a significant issue that we all have to deal with in one way or another.

Let me turn to Mr. Metcalf for an opening statement, if he wishes.

Mr. METCALF. Thank you, Mr. Chairman.

I am just going to bring up a couple questions which I brought up at the last hearing. That is whether the Constitution is involved, I don't know, but with smart cards and E-money and cybercash, the Constitution says: "Congress shall have the power to coin money and regulate the value thereof."

I am just wondering how that squares. We know that the Fed works really hard on some impact or control of the money supply, and essentially what the cards do is to monetize credit, and so how does that square with the control of the money supply?

Maybe it isn't necessary for the Fed to control the money supply. You know, we are not sure of that. But at least how does that impact this? And that would be my question or the comment I would make.

Chairman CASTLE. Thank you very much, Mr. Metcalf.

And Mr. LoBiondo?

We will wait later for his questioning period.

[The prepared statement of Hon. Floyd H. Flake can be found on page 44 in the appendix.]

We will now start with the witness, we will go across.

Obviously, if Mr. Ludwig is not here, we will skip his and go directly to Mr. Morris and come back to him.

But, Mr. Blinder, we will start with you, sir. We welcome you here.

STATEMENT OF ALAN BLINDER, VICE CHAIRMAN, BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

Mr. BLINDER. Thank you very much, Mr. Chairman.

I have submitted a complete statement and I will try to summarize it and stay within 10 minutes, if not less.

I appreciate this opportunity to present the Board's views on issues raised by various emerging electronic payments technologies

that go under names such as "digital cash" or "electronic money." While there is certainly potential for exciting developments in this nascent industry, we should all keep the latest round of innovations in some historical perspective.

First, the concept of electronic money is not new. Electronic transfer of bank balances, for example, has been with us for years. Indeed, some of the new proposals simply make available to consumers and smaller businesses capabilities that large corporations and banks have had for many years.

Second, no one knows how the industry will evolve, either in form or in size. Some of us, for example, can still remember predictions made a generation ago that the United States was on the verge of being a cashless, checkless society. Those predictions, of course, did not come true. At least not yet.

This last point reminds us that, at present, we do not know which, if any, of the many potential electronic innovations will succeed commercially. My testimony this morning will concentrate on stored-value cards and other types of so-called electronic cash, because they seem to raise the most challenging public policy issues.

In particular, depending on their design, they could amount to a new financial instrument, an electronic version of privately issued currency. But even the concept of private currency is, of course, not entirely new. Travelers checks are familiar to everyone. And in the 19th century, the United States had considerable experience, not always happy experience, with privately issued bank notes. But widespread use of private electronic currency would certainly raise a number of policy questions.

On behalf of the entire Board, I want to state clearly at the outset that the Federal Reserve has not the slightest desire to inhibit the evolution of this emerging industry by regulation. On the contrary, the Board encourages innovations in payments technologies that benefit consumers and businesses.

I am here today to raise questions and to bring some issues to the attention of Congress. It is far too soon to provide answers.

Nonetheless, it is not too soon to begin thinking about a number of interesting and complex issues that may be raised by electronic currency. And that is clearly the attitude of this hearing. These issues include the impact on Federal revenues, the legal and financial structure for these products, risks to participants, the application of consumer protection and anti-money laundering laws, and some issues related to monetary policy.

Some of these issues may need to be addressed by the Federal Reserve and other regulators, some by Congress. Some may need prompt attention, while others can wait. We believe the present is an appropriate time for public debate and discussion, a poor time for regulation and legislation.

Let me start with a potential revenue issue that will arise if the stored-value industry grows large. The Federal Government currently earns substantial revenue from seignorage on its currency issue. In effect, holders of roughly \$400 billion of U.S. currency are lending to the U.S. Government interest free. Should some U.S. currency get replaced by private electronic monies, this source of government revenue would decline. And, indeed, that is one of the major motives of the institutions interested in issuing such private

money. Because the demand for stored-value products, and the degree to which they will substitute for U.S. currency, is totally unknown at present, the loss of seignorage revenue is impossible to estimate. We believe it is likely to be small. But it is something Congress should keep an eye on.

Discussing that point raises the question of whether the Federal Government should issue its own electronic currency. Government-issued electronic currency would probably stem seignorage losses and provide a riskless electronic payment product for consumers. In addition, should the industry turn out to be a natural monopoly, dominated by a single provider, either regulation or government provision might be an appropriate policy response. But to draw that conclusion now seems much too premature. The availability of alternative payment mechanisms will mitigate any potential exercise of market power, and government issuance might preempt private sector developments and stifle important innovations.

Finally, the government's entry into this new and risky business could prove unsuccessful, costing the taxpayer money. So while we do not rule out an official electronic currency product in the future, the Federal Reserve would urge caution.

One area that may need prompt attention from both policy-makers and the industry is clarifying the legal and regulatory structure that will govern electronic money products. In this case, failure of the government to act may ironically impede rather than facilitate private sector developments.

As with other payment mechanism, issuers and holders of electronic currencies take on some degree of risk. That risk may be very small for a consumer holding a card good only for very small convenience purchases. But risk can become large when, for example, merchants and banks accumulate and exchange significant amounts of stored-value during the business day.

Risk to participants arises from a number of sources. Cards could malfunction or be counterfeited. Issuers might invest the funds in risky assets to increase their returns; and, of course, risky investments can turn sour, possibly impairing the issuer's ability to redeem the liabilities at par.

We believe that both the industry and the government should focus on answering several mundane questions that seem to be receiving little attention amid the continuing publicity about these products. For example, at each stage in the chain, whose monetary liability is the particular form of electronic money? If the issuer were to become bankrupt or insolvent, what would be the status of the claim represented on the card or balance in the computer?

Developers of such products have discussed a variety of options, but the industry does not appear to be converging on one or more models that would be transparent and readily understood by users. In addition, there is as yet no specialized legal framework for stored-value transactions, as there is, for example, for checks. From the Fed's perspective, new technological developments should not overshadow the conventional and ongoing need for clear and soundly based legal and financial arrangements in this industry.

Now, the desire to attract customers will naturally drive developers and issuers of these products to investment policies and operational controls that make their products useful and safe. So, to

some extent, the market will police itself. Nevertheless, government is very likely to become involved.

In the past, to guard against financial instability and to protect consumers, the government has followed three principal approaches. One is disclosure and surveillance, which is the procedure used, for example, in the case of mutual funds.

Another is portfolio restrictions. In some cases, standards or restrictions on assets help limit risk. Money market mutual funds and travelers checks in some States are common examples.

Third, and finally, balances in depository institutions receive the most comprehensive protection available, Federal deposit insurance.

At some point, but certainly not now, Congress will need to decide which, if any, of these protection mechanisms should be applied to stored-value products. In Europe, European central banks have gone so far as to recommend that only banks be permitted to issue prepaid cards, because that makes the balances on those cards as safe as traditional bank accounts.

The Federal Reserve Board has not viewed such a restrictive policy as appropriate. But the regulatory structure for electronic products does merit further analysis. At a minimum, we believe that issuers of stored-value cards and similar products should clearly disclose the various risks that holders bear, including their coverage, if any, by deposit insurance.

The question of whether and how to apply the Electronic Fund Transfer Act and the Federal Reserve's Regulation E to these products has received, as you know, considerable attention. Among other things, Reg E limits consumers' liability, provides procedures for resolving errors, requires institutions to provide disclosures and statements, and so on. It is possible that uncertainties regarding the application of Reg E may be holding back the development of the industry, so resolving this question would, we believe, be helpful.

H.R. 1858, as you know, would exempt all stored-value cards and a potentially wide range of other products, including transactions over the Internet, from the EFTA and Reg E. The industry appears to be worried that without such an exemption, the Federal Reserve will apply Reg E in a heavy-handed manner.

On behalf of the Board, I would like to assure industry participants and this subcommittee that we have no such intention. The Board fully recognizes that some of the requirements of Reg E should not be applied to certain of these new payment products. For example, it makes little sense to require printed receipts at vending machines.

It seems to us, however, premature to legislate a blanket exemption from EFTA without first exploring some of the basic issues raised by these new products. Disclosure policy, which I alluded to a moment ago, is a good example. If a consumer who loses a stored-value card with a balance of \$200 or \$300 is not entitled to a refund, he or she should know this when the card is purchased.

The Federal Reserve would like to develop and then put out for public comment proposals for applying parts of EFTA, such as appropriate disclosures, to stored-value cards, and for exempting

them from the remainder. We would hope to be able to accomplish this within a few months.

There are some parts of the testimony having to do with law enforcement concerns. I am simply going to skip them in deference to others that are on the panel, and to time, and come finally to monetary policy.

Concerns have been expressed that private currency might damage the Federal Reserve's control of the money supply and lead to inflationary pressures. I can assure you that this is most unlikely.

The Federal Reserve currently issues or withdraws currency passively to meet demand, and we adjust our open market operations accordingly to keep monetary and credit conditions on track. We would presumably continue to do this if private parties began issuing electronic currency, which reduced the demand for paper currency.

In any event, electronic currency, if it grows large, will be only one of several changes in financial markets in the years and decades ahead. Some of these may change the details of how monetary policy is implemented, just as financial innovations have in the past. But we believe we have the capability of adjusting to these changing circumstances while continuing to meet our traditional responsibilities for economic stability.

There is one technical issue relating to reserve requirements I want to mention briefly. Depository institutions are required to maintain reserves on cash or in Federal Reserve deposits in proportion to their outstanding transactions accounts. Under current regulations, stored-value balances issued by depository institutions would be treated as transactions accounts and hence subjected to reserve requirements. But the Federal Reserve does not currently have the authority to impose reserve requirements on non-depository institutions.

This creates a potential issue—I want to emphasize, potential issue—of disparate treatment of bank and nonbank issuers. The Federal Reserve in the past has often expressed concern about potential competitive inequities that disadvantage banks. But because of the pervasive uncertainties that I emphasized at the outset, it is far too early to have any useful insights into the implications of this disparity. We simply want to call it to the subcommittee's attention.

In summary, then, electronic payments products raise a number of diverse policy issues, both for the Congress and for the Federal Reserve. We look forward to working with Congress and with the other regulatory agencies on these matters in the years ahead.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Alan Blinder can be found on page 60 in the appendix.]

Chairman CASTLE. Thank you very much, Mr. Blinder. That has interesting insights. We look forward to being able to ask you a few questions.

By the way, just so everyone understands, I had the lights turned off. I think it is unfair to some of you, because you are very knowledgeable about this subject and studied it a great deal, to limit you too much. But I think Mr. Blinder drew up the rules pretty well when he said he would try to limit it to 10 minutes.

We do have a second panel, and when we ask questions we will go in 5-minute segments up here. And depending on how many are here, we may be able to have a second round. But we don't want to hold up the other witnesses either. So that is what we are essentially trying to do. We are not going to hold to you an exact time.

Mr. Ludwig, if you are ready to proceed, we can go to you now.

STATEMENT OF HON. EUGENE A. LUDWIG, COMPTROLLER OF THE CURRENCY

Mr. LUDWIG. Certainly. Thank you very much.

Mr. Chairman and Members of the subcommittee, I want to first commend you for holding this ground-breaking set of hearings. Given the rapid pace of innovation and the uncertainty of how these innovations will be applied and accepted by the marketplace, we absolutely must begin to think through their possible implications. These hearings make a genuine contribution in that regard.

My written statement details the evolution of these issues, and I would like to submit it for the record. I welcome this opportunity to discuss recent developments in electronic money and payment systems and the issues they raise. As the supervisor of national banks, the Office of the Comptroller of the Currency [OCC] has a keen interest in the future of money and the payment systems, both in the United States and abroad. Congress created the OCC in 1863 to oversee the establishment of a uniform national currency. Today, the OCC is committed to helping maintain a banking system that will meet the needs of the vibrant, diverse, service-based economy that will ensure the prosperity of our Nation. In addition, Secretary Rubin has asked me to serve as the Treasury Department's coordinator on electronic money issues. From both perspectives, I am convinced that steps the government takes—and perhaps equally importantly, does not take—will fundamentally influence the direction of the future of electronic money and the payments system in our economy.

The convergence of recent advances in technology and changing consumer demand are broadening the array of payment options available to consumers. One such development is electronic banking. A second development is electronic cash. A related development, often referred to as electronic commerce, allows purchasers to conduct remote transactions electronically, using the telecommunications network.

Notwithstanding the promised benefits, current developments in electronic banking have raised concerns about the adequacy of government oversight in the face of anticipated dramatic changes in the business of commercial banking. For some market participants, the changes are desirable because they signal dramatic opportunities. For others, however, the mere association of sophisticated advances in computers and telecommunication technology with banking is alarming.

Before I discuss the specific concerns associated with the development of electronic money, I think it is important for me to offer a framework that will help put these concerns into perspective. As we consider the role of bank supervisors and other regulators with respect to electronic cash and payments, we need to first remind

ourselves that these developments are only the latest phase in an evolutionary process that began centuries ago.

We can draw several lessons from the evolution of payments and communications technology. Change is inevitable, although not always rapid or predictable. While government needs to adapt to change, that adaptation should itself recognize the possibility of further change. And while government should try to anticipate problems that may arise from future changes, it cannot rely too heavily on predictions. Equally important, some of these changes may not pose new problems and therefore may not require any change in government's role.

Nonetheless, there have been and will continue to be some issues related to electronic payments that government should address. Drawing on the Administration's work on reinventing government, we have distilled four guiding principles to direct the appropriate government response: First, government should only intervene when there is a clear need to advance the public interest.

Second, when government must act, we must be careful to work with market forces.

Third, we must remember that we are public servants. Government should be extremely wary of imposing requirements solely for its administrative convenience.

Fourth, we must maintain a modern regulatory infrastructure that is adaptable to the new environment.

These principles form the basis by which we look at the emerging issues electronic commerce creates.

Innovations in electronic payments technology raise a number of important concerns, which both the government and the private sector have articulated. Of immediate concern is the need to ensure that all participants have basic information about the rules governing the use of electronic payments.

As policymakers, we must address the potential effect of increasing reliance on electronic payments on any or all of the risks embedded in all payments systems. Those risks include credit risk, or the risk of default; systemic risk, which stems from the interdependence of parties using the system; transaction risk, the risk of loss from malfunctions in the operation of a transaction or settlement system; and fraud risk, the risk of loss from counterfeit claims, unauthorized use, or misappropriation of funds.

The evolution of electronic payments technology introduces some new aspects to the continuing problem of access to banking services. We must make sure access is ensured on a fair basis for all Americans.

Another issue that further growth of electronic payments vehicles in our economy would raise is who should be permitted to issue electronic money. Traditionally, the Federal Government has retained control over money creation through its regulation of the banking industry. The potential extension of electronic money creation to nonbank firms raises many questions, including the applicability of the conventions and protections embedded in current banking laws and regulations to nonbank activity. Government would also need to address the potential loss of seignorage if electronic payments are privately issued and replace currency.

I am certain the technology to support the continuing progression in electronic payments vehicles will continue to evolve, offering many gains for all segments of our economy.

Ultimately, the market will decide whether these innovations succeed, and whether electronic payment vehicles will come to dominate the payments system. Government's role is to protect the public interest, ensure the efficiency and competitiveness of our markets, and maintain public confidence in our financial institutions and payments system. As Comptroller and coordinator of the Treasury Department's effort on electronic payments issues, I am committed to ensuring that we carry out that role efficiently—in conjunction with market forces and ensuring that the public interest is protected.

I look forward to working with you, Mr. Chairman, and the Members of your subcommittee on these matters.

Thank you very much.

[The prepared statement of Mr. Eugene Ludwig can be found on page 48 in the appendix.]

Chairman CASTLE. Well, thank you very much, Mr. Ludwig. We appreciate your being here and your comments and look forward to having a little discussion with you later on.

And next is Mr. Morris, who is the Director of Financial Crimes Enforcement Network.

STATEMENT OF STANLEY MORRIS, DIRECTOR, FINANCIAL CRIMES ENFORCEMENT NETWORK

Mr. MORRIS. Thank you, Mr. Chairman.

I, too, would like to congratulate you and the other Members of this subcommittee for setting up these timely and very important hearings. And we are very pleased to participate.

I would like to summarize briefly the full statement that I have submitted to the subcommittee.

As you mentioned in your opening remarks, 2 weeks ago we sponsored a colloquium at the on-site repayment systems at the New York University School of Law, where we brought together approximately 125 people to address the evolution of advanced electronic payment systems.

The message we received from that colloquium, as well as from our industry-based Bank Secrecy Act Advisory Group, is the very one that you heard in July and are hearing again today. And that is advances in the design and implementation of the new payment systems are among the most complex and potentially far-reaching developments generated by the age of the intelligent machine.

What are the elements of the new systems that cause concerns for officials responsible in our situation for fighting money laundering and financial crime? This is what I would like to address to the subcommittee this morning.

First, however, it is important to emphasize that the fact that we are thinking about the new technology does not mean that we are against it. Indeed, just the opposite. It means that we are keenly aware of our need and of our responsibility to understand the technology first, before deciding if there are law enforcement issues that require attention.

Our interest in the new systems reflects our own responsibilities as a regulator. The Bank Secrecy Act, for which we are responsible requires the recordkeeping and reporting of some 200,000 financial institutions of all kinds, creating for us the largest currency transaction recording system in the world. And we have already begun asking whether and how that act, the Bank Secrecy Act, applies to these new systems.

That range of issues is another reason we are involved. As our name indicates, FinCEN itself is a network. FinCEN tries to bring enforcement agencies and the private sector together wherever it can to create cost-effective measures to prevent and detect and deter financial crime.

We are keenly aware of the potential impact that the new technologies can have on the work of financial investigators. Let me explain.

Financial investigations are recognized as the key to combating narcotics trafficking and organized and white collar crime. Such investigations are difficult to carry out. The sheer size, variety and pace of change in the financial sector makes financial investigations perhaps the most difficult aspect of Federal law enforcement today.

Our strategies to deal with these difficulties have historically centered on eliminating bank secrecy, where it aids and abets criminal activity. And Treasury has administrated that—administered the act, I believe as Congress intended, to require record-keeping that would preserve a financial trail for investigators, and to require reporting of significant currency transactions, and transportation of currency and monetary instruments across our borders.

Over the past 2 years, building on legislation which originated in this subcommittee, we have worked to “reengineer” the Bank Secrecy Act, enlisting support of industry, cutting out unneeded regulation, and trying to simplify what remained.

The investigator’s motto, “follow the money,” relies on the need of criminals to move funds through the financial system, to hide and use the proceeds of their crime. Currency is anonymous, but it is difficult to handle and transport in large amounts. Anyone who has seen a pallet of newly printed bills at our Bureau of Engraving and Printing, or better yet, has seen a photograph of a drug cartel’s counting houses or currency stashes, knows exactly what I mean. A large amount of currency is like an elephant, it is difficult to hide. It takes time to move, and it attracts attention. And attention is the enemy of criminal activity.

The new payment systems have the potential to change all of that. If cards can be “loaded” with value not just from banks, but from other retail outlets or from other sources, current systems for tracking funds could lose their value. Internet-based systems for transferring large amounts or a way to store large sums on a “smart card” that would be recognized as “carrying” dollars at any place in the world, clearly pose some risks.

In short, the new systems combine the speed of the present-based bank-based wire transfer system with the anonymity of currency; they create potentially the best of both worlds.

Is that necessarily bad? Not at all. In fact, far from it. At the colloquium, my boss, Under Secretary Noble, used an example I would like to repeat today: A U.S. retailer, let's say, a shoe store, could accept smart cards for purchases. As the store's revenue increased, it could transfer the value of its revenues to a smart card or download the value into a computer. The value can in turn be transferred over the telephone lines or through the Internet to financial institutions or people around the world, to pay invoices, order materials, pay suppliers. In all cases, stimulating commerce, making trade less expensive, providing benefits to consumers.

The same systems can benefit consumers in other ways. They can reduce the hazards, and inconvenience of carrying cash. They can provide a significant degree of protection via smart card technologies, for those who are unbanked, who do not have bank accounts. They can foster electronic commerce and they can reduce the cost of processing cash by retailers and the risks of robbery for merchants in many of our inner cities.

But the same efficiencies could, at least in theory, create opportunities for serious exploitation by money launderers. Suppose my Internet user is a narcotics trafficker or an agent for a gang of sophisticated criminals. Consider the invoices the trafficker might pay, the supplies he might order, the transactions he might accomplish, if, for instance, he could download an unlimited amount of cash from a smart card to a computer, and then transmit those funds to other smart cards in locations around the world, all anonymously, without an audit trail, and all without the need to resort to a traditional financial institution.

History has shown us that as we invent new technologies, criminals are waiting on the periphery to use them. Trains produced train robbery, telephones create telephone frauds, aircraft—hijacking, terrorism, and the like. In the same way, the possibility of virtually untraceable financial dealings, if it were to come to pass, could create new, but this time, perhaps unparalleled problems for law enforcement.

Those of us who have fought hard to end bank secrecy as a convenient excuse around which criminals can cluster, will have won little, if we now turn to a world in which financial institutions can easily be bypassed via the Internet or the use of telephone lines.

That leads to an important point about money laundering and related financial crimes. They all involve taking acts that are themselves, in isolation, not only legal, but commonplace, opening bank accounts, wiring funds, exchanging currencies in international trade. Given that basic fact, we have few ways now to separate the malefactors from the honest businessman. The new technologies could give us even fewer ways, unless we work with the industry as the industry develops.

How shall we do this? I tell you frankly, we don't have an answer. Technology raises the stakes in many ways, and for each risk, there is clearly a benefit. Or the reverse, for every benefit, there is a risk.

We would be concerned if the new systems permitted encryption, for example, of large financial transactions in a way that would make their detection or their identification of the sending or receiving parties impossible to reconstruct. But encryption is vital to pro-

tect the security of electronic commerce and financial transfers, and sophisticated encryption is already in place of course in the interbank transfer systems. And we recognize the use of encryption and its importance in protecting privacy where consumers feel they may be threatened in the computer age.

We are not without tools to deal with issues as they develop, although, frankly, we don't know yet whether these tools will be adequate. BSA authorizes the Secretary of the Treasury to require recordkeeping by financial institutions and to require reports of suspicious transactions and currency transactions. It also requires the registration of money transmitters.

How do these concepts apply to these new systems? Here are some questions that we are asking the industry today: Do the systems create and maintain an audit trail?

Does that trail extend beyond the initial transaction to subsequent transactions in the chain?

What are the privacy implications of that audit trail?

Will the systems be restricted to transactions below a certain dollar amount, a cap, if you will?

Will the systems permit effective and timely monitoring of suspicious transactions? For example, repeated multiple transactions to evade dollar caps.

Are cyberpayment systems to be offered by or through a regulated financial institution?

Do the systems permit self-contained, person-to-person transactions without the involvement of a financial institutions?

We may need this subcommittee's assistance in dealing with these questions, but the time, as the chairman has pointed out, and as I think both the Federal Reserve and Mr. Ludwig have pointed out, the time right now is to ponder these questions, not rush to solutions. Too often, government regulators have attempted to thwart a potential criminal threat by imposing burdensome regulations that reflect little appreciation of the nature of that threat, or the business practices of the affected industries.

We cannot make the same mistakes with these new systems. The technology is developing too rapidly, and the gains in efficiencies potentially created by the systems are too important. But without thoughtful and balanced approval of law enforcement concerns now, before criminals begin to exploit new technologies, the prospects for abuse by organized crime, money launderers and other financial criminals could be too great.

What does the "cyber-future" hold for us, those of us responsible for money laundering? Quite candidly, we haven't figured that out. We are working closely with the Comptroller of the Currency; as he pointed out, Secretary Rubin has asked him to coordinate Treasury's broad efforts in this regard. And we have recently worked with the Defense Department's Advance Research Project Agency which has awarded an account to KPMG Peat Marwick, to assist us in understanding the dimensions and developments in this industry.

I hope that FinCEN can serve genuinely as a "network," as we tried in the colloquium 2 weeks ago to enable all of us in law enforcement, financial, compliance officials, technology developers,

the bankers, to try to work out the details and solutions to some of the potential problems that I have outlined.

We want to advance, not impede, the development of technologies that can benefit us. Our goal is simply to inoculate such systems if we can against crime and misuse by criminals, to permit the healthy growth in the best public interest.

So our task is just beginning and we look forward to working with you and Members of this subcommittee in that spirit.

Thank you.

[The prepared statement of Mr. Stanley Morris can be found on page 74 in the appendix.]

Chairman CASTLE. Thank you very much, Mr. Morris.

Before calling on Ms. Katzen, we will have a second panel after this, we will have questions of you before we go to the second panel. The panels are of equal stature. It is just we couldn't handle eight people all at the same time or the questioning would be unfair to the Members. So that is the reason for the division.

And finally, we will hear from Sally Katzen, who is the Administrator of the Office of Information Regulatory Affairs, the Office of Management and Budget.

Ms. Katzen.

STATEMENT OF SALLY KATZEN, ADMINISTRATOR, OFFICE OF INFORMATION AND REGULATORY AFFAIRS, OFFICE OF MANAGEMENT AND BUDGET

Ms. KATZEN. Good morning, Mr. Chairman, Members of the subcommittee.

And despite the long title, I am here in my capacity as Chair of the Security Issues Forum of the Information Infrastructure Task Force that was convened by the Vice President and chaired by Secretary of Commerce Ron Brown. The Forum is the interagency group that is responsible for coordinating and articulating the Administration position concerning security of electronic information.

And before I begin, I, too, would like to commend you for having these hearings. I think they are an important part of the process, and I was particularly struck by your decision, which I think is eminently correct, to have the first hearing devoted to hearing from people in the private sector before you heard from the government administrators.

I think that is useful because the private/public discourse is probably more important in this area than in almost any other. And starting with the private sector was, I believe, a good move.

I, too, have prepared a written statement which sets forth a brief history of what the Clinton Administration has done, the work it has done to explore and carry out government's responsibilities in the area of security of electronic information.

Having heard the previous witnesses address, as you would expect them to, issues having to do with financial institutions and monetary policy, and recognizing that we are obviously here in this committee room thinking about the implications of electronic media for banking and related industries, I would like to use my oral comments to try to provide a somewhat broader perspective. Because as important as the banking and monetary and financial institutions piece of this is, it is just a piece of a larger picture of the use

of electronic media for the transmission of information and data, as we will see.

Now, we are talking about the growth of high-speed telecommunications networks, databases, and advanced computer systems which are called the NII, the National Information Infrastructure, that is going to provide information widely, make it widely available and accessible. And we expect the NII will provide a host of benefits in this field and others. But as we open our networks and we increase our interconnectivity, we must confront the questions of security in the NII.

Now, what do I mean by security? Frequently it is viewed as synonymous with confidentiality. That is, assuring that the information will be kept secret, with access limited to appropriate persons. But when we talk of security and as you think of security, I hope you think of it in the broader sense of going beyond confidentiality, to include the integrity of the information, that it has not been tampered with along the way; the availability, it is there when you need it; and reliability, that the systems that are transmitting the information or providing the transactions continue to function.

It seems to me that there are two major questions that we should focus on. One is how to achieve and maintain security in the NII? And the second is what is the government's role in that effort?

The first, achieving and maintaining security, is largely a matter we think of identifying the risks and vulnerabilities introduced by the use of new technologies to do business electronically. In other words, create an inventory of the needs of the users and providers of services. Then if we unleash the incredible talent in this country, some of which is in the government but most of which is in the private sector, we can solve the vast majority of the technical or operational issues through a combination of hardware, software, management techniques, training, personnel.

And so it is the second question, which is what is the government's role, that I think is the real public policy issue that I have been focused on, and that I would like to speak to this morning. The Administration is clear that the NII will be designed, built, owned, operated by the private sector. But the government will be a major user of the NII. And it also has a responsibility for being a facilitator or catalyst in creating the legal and policy framework within which the full potential of the NII can be developed. So there are governmental responsibilities.

But I would like to echo the words of some of the earlier witnesses, they are limited. In order to better understand the parameters of the government's role, we published in June in the *Federal Register* a paper that attempted to describe the need of security to the NII and what the appropriate governmental responses might be. We are now analyzing the comments that we have received.

And I would say that generally our paper was well received. There is no dispute that there are, in fact, areas in which the government has a legitimate role. But it was also clear from the comments that many people believed that the government's role should not be very intrusive, that the marketplace itself will provide the security that we need in this field, as in others.

Let me draw, if I can, on two areas of interest to this subcommittee that have been mentioned by earlier witnesses or in my written

testimony. The first involves the government's use of the facilities as a user, and that would be the Electronic Funds Transfer, EFT, and the Electronic Benefits Transfer, which no one has yet discussed, but I think is a very important aspect of the government's use in providing benefits electronically.

The second involves our duty to protect and provide for the national defense and economic security. Now, on the Federal use of the NII for the distribution of funds or the distribution of benefits, it is clear that electronic distribution is safer, more cost effective than traditional paper means. At the same time, it introduces a host of risks which have been addressed by some of the other witnesses and were mentioned in the opening statements.

Now, the government interest is real here because we are a user. But I think it is significant that consistent with our emphasis on a private/public partnership, we have decided to rely almost exclusively on commercial private and public networks for our electronic transactions. And that means we will not build a new infrastructure to support EBT. It will not be a government-owned infrastructure.

We will instead rely on the existing debit network infrastructure to meet our operational needs. Similarly, we expect to rely on the private sector for meeting the security needs attendant to that electronic transmission.

It is our hope that EBT and EFT efforts will serve as laboratories for improving reliability and safeguards in the NII generally.

Now, the second reference goes to our act being as a regulator rather than as a user, a formulator of policy. This is significant because as the United States becomes increasingly reliant upon the NII, key sectors of our economy will be inextricably tied in and hence dependent on it. I am referring here to the power grid, our transportation systems, our weather system, financial institutions, which increasingly will become dependent on the NII.

A security weakness in one of these areas can place other elements at risk. And a significant attack on the NII would be a threat to our national and economic security, in addition to the significant personal and economic harm it would cause. Thus, the stakes are very high and the Federal entities that oversee various parts of the U.S. economic infrastructure must be aware of the new risks, their magnitude, and possible solutions that they can provide in their overseeing capacity.

We must approach this role of overseer and regulator as taking as our first principle, "do no harm." And I was pleased to hear that some of the earlier witnesses echoed that theme for their own area. This is a very dynamic economy and we must not needlessly inhibit its evolution by micromanagement.

I think you have heard today from some of the witnesses from Treasury, and from Mr. Blinder, and you will hear from others of how we are beginning to look at the regulations to ensure that security will be a part of it. But in both of these instances now, as user and as regulator, I come back to the theme that our success will depend on a good private/public dialogue.

We are attempting to cover this through our series of public meetings that we have held, and through our U.S. Advisory Council on the NII. And we have found that one area where such dia-

logue is particularly necessary is the area of encryption, cryptography. The Banking Committee has been a significant user of strong cryptography to protect its transactions for a long time and will for the foreseeable future.

Indeed, one of your witnesses at the July hearing pointed out that cryptography is the enabling technology to secure financial transactions, including digital cash of the future, as it protects both the confidentiality as well as the integrity of the information. At the same time, you have heard and you will hear in the next panel that strong cryptography can thwart law enforcement's legitimate ability to understand the contents of the information that it may obtain either through lawful wiretaps or lawful searches and seizures.

A number of years ago, we as a society decided that for public safety reasons, our law enforcement agencies must have the ability under tightly controlled procedures, to listen to certain electronic communications or seize properties such as stored data.

We cannot unnecessarily impede or impair that public safety capability, and so we must strike a balance between the public safety and national security implications of strong cryptography and the need for privacy and business confidentiality of our citizens and businesses in an international marketplace.

It is important therefore that we as a society have an informed, rational dialogue about this important subject and reach consensus on how best to solve it.

Mr. Chairman, in my role as a coordinator of executive branch regulatory activity, I have developed an acute appreciation of the value added by extensive public participation and development of governmental policies. This area is no different.

Given the importance to the Nation's economic future, the potential impact of government activity on our most vibrant industries, and the complex privacy and liability issues that can arise, it is essential that we engage the public early on in our deliberations. As my written testimony shows, we are doing that in the executive branch, and I am delighted that this subcommittee is taking the lead in the legislative branch.

Thank you very much.

[The prepared statement of Ms. Sally Katzen can be found on page 85 in the appendix.]

Chairman CASTLE. Thank you very much. I endorse your philosophy, do no harm. That is a good philosophy for government at all times.

I was struck about a month ago, when we had a demonstration to various Members of our committee of the new \$100 bill, of the interagency cooperation among the different government agencies in putting that together, those who worry about security, those who worry about physically putting it together and all the implications of that.

I was also struck by the fact that that group seemed to be anticipating problems and had an understanding that probably in the future we will have to change our bills even faster than we do today because of reproductive equipment advances and things of that nature.

I thought it was very futuristic thinking for government in particular, and I am struck today by the testimony of the four of you that you have already given a lot of thought; there has been a lot of thought given to exactly what we are dealing with, and I hope and I am sure you are already coordinating this, which is hopefully something we can facilitate, because it is vital that we help each other with this, because it is a brave new world, as I indicated early on, and I think we need to be concerned about it.

We will now enter into a period of answering questions. We will have a clock running for the various Members, and that means that—my time is almost up—that means that we may not get through all the questions.

The things that you have stated have provoked many, many questions, more than we can take the time to answer right now, because we do want to get to the next panel and allow them to testify, but we may want to submit questions to you in writing if you would be kind enough to get back to us at some point.

Let me start the questioning, if I may, and ask you a question directly, Mr. Blinder, on the subject of possible exemption. You mentioned it, and I was going to ask it anyhow.

I don't know the legislation you referenced particularly, but I do know that under Regulation E of the Electronic Fund Transfer Act, any issuer that provides consumers electronic funds transfer services has substantial compliance responsibilities, and I understand that home banking is covered by this relation.

I got to thinking, should there be smart cards and electronic cash at minimal levels that should be exempted from this? Apparently the legislation you referenced, H.R. 1858, would exempt certain stored-value cards. I was curious as to your thoughts of the merits of such legislation. I am not familiar with it in particular, but the concept—we saw demonstrated here, for example, \$20 cards that you could use in a vending machine or telephone, and I am not sure if this enters into the same level as General Motors electronically transferring cash or whatever it maybe.

Mr. BLINDER. I think you have put your finger on exactly the question that is on our minds. It is easy to imagine that extensive exemption, if not indeed blanket exemption, from these requirements would be appropriate for a \$20 stored-value card.

If you start thinking about the equivalent of cash passing computer to computer over the Internet, involving possibly large sums of money, or even stored-value cards involving substantially larger sums of money, I think it raises some questions about whether blanket exemption is obviously the right strategy.

We certainly would not imagine that these sorts of products should be regulated exactly as if they were credit cards. They are not credit cards; they are quite different; and they are used in different ways.

One of the problems is, when we say "they," we don't know what kinds of objects we are talking about because they are not yet in existence out there. It is for that reason that the Board took the position back in May, and still has the position, that we would prefer not to give total blanket exemption to these activities, but rather to try to think through, after a public comment period, in which we would hear from actual and potential participants in these ac-

tivities, what are the appropriate parts of the EFTA to apply, what are the appropriate parts not to apply, what needs modification for these technologies—which were not, I don't believe, what Congress had in mind when it passed the EFTA years ago.

Chairman CASTLE. A basic question that I would like to ask you: You said it, and it is a known fact, electronic transfer of dollars is not new. Big banks and big corporations have been doing this for years, the use of Internet and use of home computers. Can you define for me precisely what it is that is starting to happen in 1995 that did not exist, say, 5 years ago that we need to be concerned about, not necessarily regulating, but be concerned about?

Mr. BLINDER. If I may escape the word "precisely," I will answer. The reason we focused, in preparing the testimony, on products that, I guess, can come under the rubric "stored-value" is that they look a bit different from other forms of electronic banking. Familiar forms of electronic banking amount to ways to do standard banking activities—taking deposits, making payments, even making loans—through electronic means rather than face-to-face or with a paper. It is taking familiar transactions and giving them a different form. We focused the testimony on stored-value products because these seem to be creating private electronic currency, which is a somewhat different object, to our way of thinking.

Chairman CASTLE. A final question of you. You indicated in your testimony that it is unlikely that these kinds of transactions might damage the currency supply, and you said there would be a lot of other changes ahead.

It is so hard for newcomers to grasp what this could entail, but it seems to me that the exchange of value over the Internet by millions of unidentified individuals and businesses would at least affect the ability of the Federal Reserve to monitor monetary policy and monitor currencies outstanding, and I would think that you would have a great deal of problem following all this—Mr. Morris has alluded to this too—following all this in terms of the money being created and where it is.

I view that as being perhaps more of a threat than I thought you had indicated in your statement. If you could relieve my concern about that, I would appreciate it.

Mr. BLINDER. Let me try to clarify. In our mind, there are two major questions about this industry, and of course we don't know the answer yet, and neither does anyone else.

How large will it grow? If this activity—stored value liabilities of banks or nonbanks that don't look like Federal Reserve notes but function as currency—never grows very large, it is not something that we would be worrying about for monetary policy.

We now have travelers checks, about \$9 billion in outstanding travelers checks. That is small relative to any measure of money supply. So question one is, will this ever grow to be a very large share of the total media of exchange? We don't know the answer to that. It is possible that it will. But it certainly will not in the short run.

Second, what fraction of this activity will take place through banks as opposed to nonbanks? For obvious reasons having to do with reporting and supervision, we have a lot more information

about what happens in banks than we do about what happens in nonbanks.

Again, nobody knows the physical locus of this industry as it will evolve in the future. If it is all inside banks, it will be reported to us, just as banks report other sorts of deposits and activities. If a great deal is done outside banks, it will not be.

If those two questions both get answered in particular ways, then this could grow to be a greater problem than I indicated. That is to say, if the industry grows extremely large so it gets to be a very significant share of the payments mechanism, and if a great deal of that activity is outside banks, then I think that would pose some problems for the Federal Reserve. We don't know if that will ever happen, and we don't believe it is on the near-term horizon.

Chairman CASTLE. One quick question. In the formation of dealing with this issue of electronic currency, do you think there should be exclusions on nonbanks being involved in it? Do you think it should be funneled through the banking system?

I am not thinking of individuals now but of the different corporations that deal in finances and in banking practices, even though they themselves are not banks, of which there are a number in this country today.

Mr. BLINDER. Given the pervasive uncertainties, and given how nascent the industry is and that some of the innovations seem to be springing from outside banks, we don't recommend that policy now. Sometime in the distant future we don't know what we might think, because we don't know what is going to happen between here and there. But we think it would be a mistake, and do not advocate at this point, restricting the activities to banks.

European central banks have taken a different view of this, as we mentioned in the testimony.

Chairman CASTLE. Thank you.

Mrs. Maloney.

Mrs. MALONEY. Thank you very much.

The *New York Post* today and yesterday has been highlighting waste and abuse and mismanagement in the Federal food stamp program, citing a Department of Agriculture audit. There are certainly too many people who rely on this important program, and funds are too scarce for any abuse to be tolerated.

Could any of you give me specific examples of how we could use this new technology in programs like the food stamp program to prevent fraud and to make it a more accountable program?

Mr. LUDWIG. I am quite concerned about the consumer well-being aspects of the technology, but at the same time there are tremendous potential consumer benefits.

Let me analogize to banking. If you just take the cost of a paper-based system, for example, where a teller's involvement can cost on average in the United States as much as \$4 per transaction, versus the cost of going to an electronic-based system, which can be pennies, there are savings that can be passed on generally throughout the system. In terms of security, there are potential benefits in terms of what value electronic value cards might have if they are stolen.

But as Vice Chairman Blinder said, this is a very nascent area, and the degree to which these problems will be solved or amelio-

rated, and the degree to which there will be other problems created, will not be entirely clear until we see how the technology develops.

I know the Financial Management Service is testing electronic benefit transfers to about 20,000 people in Texas. As you have suggested, there is hope that fraud can actually be decreased.

Mrs. MALONEY. How could it be improved? How would it be a better system in fighting fraud?

Ms. KATZEN. There is some information from the Maryland Freedom Card that USDA did a final evaluation on and determined that the benefits diversion was approximately 42 percent. That is a significant number.

Aside from the cost savings Mr. Ludwig mentioned that can help the system as a whole, if you are able to significantly reduce the amount of diversions either because the food stamps get lost beforehand or never reach the recipient or then are not used in the proper way, that number is quite significant. It is only one, but it does show that among steps from the very beginning until the time it is actually used, there are a number of points where benefit diversion can be restricted through electronic means.

Mrs. MALONEY. They cited that vendors are abusing the system so people with food stamps are buying bicycles and beer as opposed to food. How would an electronic benefit transfer card prevent that if a vendor is fraudulent?

Ms. KATZEN. The Electronic Benefits Task Force has been putting together a series of building blocks, which includes not just the distribution but also the use and the audit principles. You will have in some instances better records that are less burdensome to maintain in terms of being able to construct an after-the-fact audit of some of the uses.

It is not a panacea, it will not solve all the problems, and I will not sit here and tell you that if it were universally used there would be no fraud, there would be no diversions, but I think there are a number of areas in which we have seen already in the pilot projects which are existing at the city level, at the State level, and consortiums of States, that there are in fact heightened protections to and including the audit trails.

Mrs. MALONEY. They also cite—I believe they said \$85 billion in New York State was wasted because people who were ineligible received food stamps. Again, how would the electronic benefits—

Ms. KATZEN. That would not affect that. We are talking about a delivery system. Assume whoever is supposed to make the eligibility determinations, assume whoever is supposed to determine how much money goes in, this is the way you deliver it to the beneficiary, and in that regard there is a part of the trail that can be protected, if you will, but it is not going to be able to solve all the problems.

Mrs. MALONEY. Mr. Blinder, would you like to comment?

Mr. BLINDER. I have nothing to add. I must admit that we have been thinking more about conventional financial issues than about food stamp fraud, I am sorry. I don't disagree with anything that has been said, however.

Mrs. MALONEY. Thank you.

Chairman CASTLE. Thank you, Mrs. Maloney.

Mr. Metcalf.

Mr. METCALF. I want to thank this panel for a very interesting discussion and answers. My first question is to Mr. Blinder.

You mentioned the \$400 billion in Federal Reserve notes that is outstanding and the seigniorage issue, and of course we are very much interested in that issue, relative to the dollar coin bill that we have here which I hope passes eventually. You said something, that these Federal Reserve notes related to lending to the U.S. Government interest free. Those were your words. Explain that a little bit to me.

Mr. BLINDER. What I meant by that is that people that hold Federal Reserve notes—and that is all of us—are holding a paper liability of the U.S. Government, in this case of the Federal Reserve, which does not bear any interest—as compared, say, to a Treasury bill, which many people hold, and does bear interest. The fact that they don't bear interest makes them a revenue source to the government.

Mr. METCALF. I was thinking of the Treasury separate from the Federal Reserve and interest is paid directly on those Federal reserve notes.

Mr. BLINDER. It is not wrong to think of the Federal Reserve and Treasury as integrated in this respect, although we are formally separated, because our earnings on these things are turned over to the Treasury and therefore become taxpayer property.

Mr. METCALF. Mr. Ludwig, maybe this is the same kind of thing. You said the government would have to address the issue of the loss of seigniorage as we move toward the electronic money. You were referring to the same thing that he was referring to, loss of seigniorage essentially to the Fed?

Mr. LUDWIG. Yes, sir. As the technologies are now nascent, there is no question, but if they became enormously robust, there would be an economic impact to the Federal Government and that would have to be addressed one way or the other.

Mr. METCALF. If the Fed gets seigniorage on the bills and the U.S. Treasury gets the seigniorage on the coins, which is interesting.

My second question; the Office of the Comptroller was established as you mentioned to regulate the U.S. notes that were issued in the 1860's, I think you have said. How do you explain the fact that Congress specified a certain dollar amount of U.S. notes remain in circulation, and yet today no U.S. notes are in public circulation?

Mr. LUDWIG. That is interesting. I will try as best I can to answer your question verbally, but I should give you a written response.

Mr. METCALF. I would like that.

Mr. LUDWIG. I will definitely do that.

[The information referred to can be found on page 158 in the appendix.]

As you well know, the system has changed dramatically since 1863, but there are bits and pieces of it that have not changed, for good or ill. For example, until 1994 I had legal responsibility for approving the plates for all the bills, even though in fact the real responsibility for the currency had been passed to others long ago.

Similarly, the requirements in terms of what is in circulation is a complex set of rules that have changed over time.

Mr. METCALF. I believe that this is clearly a violation of Congressional intent to hold these notes apparently in vaults somewhere, but technically saying they are in circulation. Since the U.S. notes, like the coins, the seigniorage accrues to the U.S. Treasury directly, I think that is something that we should think about. I think they should be taken out of the vaults and circulated along with the Federal reserve notes today. I would just like to implant that thought there. I appreciate your comments. Thank you.

Chairman CASTLE. Thank you very much, Mr. Metcalf. Just a quick follow-up, a couple of questions.

Mr. Morris, the whole business of the \$10,000 reporting threshold that we have now, which I think is very significant in financial law enforcement, I think keeps a lot of people from getting away with things they might otherwise get away with. I am concerned that if we set up an Internet system and an exchange system that we could start to get electronic transfers in excess of \$10,000 and maybe from without to within the country and vice versa. It raises in my mind the specter of potential problems like that. Where are we going with respect to that issue?

Mr. MORRIS. Mr. Chairman, our regulatory responsibilities are really twofold. One, they regulate banks to maintain certain kinds of currency reporting and recordkeeping, and we also regulate transactions across our borders. Any system that eliminates currency and banks from that equation obviously eliminates the tools that we have to deal with money laundering. So you are correct.

The systems that we have put in place in very close partnership with related financial institutions have made currency less anonymous. Money laundering is a more difficult criminal activity now than it was 10 years ago. Indeed, the costs that we see from activities in undercover operations and the like have increased significantly; that is, the cost to criminals to get their dirty money into clean-appearing monies is much more costly than it was a few years ago because of those systems. So clearly any systems that come up that could eliminate the progress that we have made would be a problem.

I would like to make one point here, though. I think we have also fallen into language in talking about this as an industry. I am not sure it really is an industry yet. Indeed, when we put together the colloquium, we talked about the various service activities that were going on. Many of these are really new procedures within existing industries. They are applications of new technologies. So it is very hard for us to get our arms around exactly what it is we are dealing with potentially.

In many cases, we are talking about a consumer convenience, a card with low amounts of cash on it as the MONDEX system in Swindon, England, which is closely associated with banks. These systems are of very little interest to us. But these same systems in fact expand into areas that would have significant interest to us.

You are correct; if we were to go to situations where large amounts of money could be loaded onto smart cards and put between cards over the Internet or over telephone lines, then we would provide a license to steal for criminals around the world.

Chairman CASTLE. One final question, and that is, is electronic commerce a matter of sufficient national importance that Congress should preempt the field and prevent States from adopting or enforcing conflicting legislation? Not that the States are threatening to do anything but at some point that may come up as an issue. If you have an opinion on that.

Ms. KATZEN. I would say that it is hard to answer that now, in part because what we are seeing is a number of laboratories at the State level, indeed at the local level. There may be areas where it will be necessary to have some Federal law.

We had just recently, for example, in an unrelated field issued a report on protection of intellectual property rights in the NII and suggest some changes to the copyright statute that would address some of the issues rather than leaving it to the States. But I think at the current time we would suggest a more let's watch what is happening rather than rush in and try to set some ground rules right now.

Chairman CASTLE. Thank you. Ms. Roybal-Allard has joined us.

Ms. ROYBAL-ALLARD. Thank you.

The district that I represent is in an urban area containing a predominantly low income and minority population. The district already suffers from the lack of financial institutions providing traditional financial services and products which leads to one of the concerns that I have with the advent of electronic cash. Will there be an even greater gap between the haves and have-nots in terms of the availability of these services to these communities?

Mr. LUDWIG. I might take a shot at that. It really remains to be seen, as I said in my testimony. We have to ensure that people of all economic groups are treated fairly and that access is available. The new CRA regulations which we worked on accommodate this new technology in several ways, so we have been mindful of that. But, there are some facts which suggest that the new technology might actually provide greater access as opposed to less access.

Interestingly enough, although I think it is generally perceived that the number of bank branches in this country has gone down while ATMs have gone up, in fact, there has been a net increase in bank branches in this country, while ATMs have skyrocketed. So, although there are dire predictions of branches disappearing, that hasn't been the case to date.

Moreover, there are a lot of problems that electronic money could solve for low- and moderate-income individuals. As I said earlier, the cost of a teller transaction is on average in this country about four bucks. Since the cost of electronic transactions can be pennies, there are savings that can be passed on generally throughout the system. In addition, we currently have individuals with government checks going to check cashing outlets and being charged very large amounts of money to cash those government checks. Electronic transfer can not only be efficient in terms of costs both for the consumer and the government, but it can also eliminate or diminish that charge. A lot of the electronic activity that is taking place goes on over the telephone, and almost everybody in America, including low- and moderate-income individuals, has a telephone and can access it.

So, I think we have to be watchful and concerned since this is a very nascent set of technologies. We don't know exactly how they will develop, but there is some reason to believe that they will be beneficial for low- and moderate-income individuals, as well as the rest of society.

Ms. ROYBAL-ALLARD. I apologize for not being here for the testimony so my next question may have been covered. When I was in the California State Legislature, one of the arguments used by banks as to why we should support ATMs was the fact that it would save the customer money. At that time the services were free and there were all kinds of arguments made on how this would be better for the consumers; it would be cheaper, and so forth, than having to use a teller.

As ATMs became more popular, the banks started charging for the service that was originally free and which was the basis of the argument in order to get the State legislature to support them.

What is going to happen in terms of the electronic cash if the fee is low now but then becomes extremely popular? How will the costs be controlled or will we see the same thing happening as we did with ATMs?

Mr. LUDWIG. I would suggest that the teller cost is not merely, or maybe even significantly, a function of the ATM technology as an alternative delivery system, but of a general increase in the cost of the utilization of these physical facilities. My suspicion is that if we are going to look at an efficient delivery system that really can keep consumer costs low, we have to be able to modernize in an electronic direction. If you look at it this way, the cost of electronic transfers, or the cost of computer services, has decreased by half every 18 months over the last 20 years. It is really phenomenal that the cost of computing has decreased so much. These computing costs are getting very, very low, and at the same time the cost of personnel has increased. It is a mix, really, of the utilization of peoples' talents, and the utilization of these new economic means, that is likely to benefit consumers through lower prices. But, to try to restrain technology or to try to require that we use a branch-based delivery system only is likely to drive up costs.

Ms. ROYBAL-ALLARD. Thank you.

Chairman CASTLE. Thank you very much.

Let me thank this panel a great deal. You have helped I think further our knowledge in this area and hopefully the resolution if any is needed of what we have to do.

We will hear from the next panel. We have four witnesses and I will go over who they are.

Mr. Kammer is the Deputy Director of the National Institute of Standards and Technology. Mr. William P. Crowell is the Deputy Director of the National Security Agency, also known as NSA. Philip Diehl is the Director of the U.S. Mint. He has appeared before us on a number of occasions in a variety of roles. Robert Rasor is Deputy Assistant Director for Investigation, Secret Service. Welcome.

We apologize for having to divide the panels up. The panels are of equal significance, but we had to do it in order to get questions in and giving the Members an opportunity. With that, Mr. Kammer.

**STATEMENT OF RAYMOND G. KAMMER, DEPUTY DIRECTOR,
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**

Mr. KAMMER. Thank you, sir.

As you said, I am Ray Kammer, Deputy Director of the Commerce Department's National Institute of Standards and Technology. Under the Computer Security Act of 1987 and the Paperwork Reduction Act of 1995, NIST is responsible for developing and issuing standards to protect unclassified government computer systems.

In response to the topics which the committee expressed an interest in, I thought I would focus on four concepts today: First, give you an overview of encryption and digital signature technologies; mention some of the risks and hazards of using encryption; bring you up to date on some of the government's activities to find key escrow solutions that would balance the requirements of users with the need for law enforcement and national security; and finally discuss a bit the importance of taking a system-wide approach.

There are two important technologies I think here. Encryption protects the confidentiality of information and digital signature helps ensure its integrity.

One of the most widely used encryption algorithms is the Federal Data Encryption Standard that was published by NIST.

We have also published standards for digital signature and for some of the enabling technologies that are necessary to use a digital signature.

The benefit, of course, of encryption is confidentiality. With digital signature you also get a basis for the recipient of an electronic transaction to be certain of the identity of the originator and also of the integrity of the message. To my thinking, there are five attributes that are necessary for full electronic commerce and four of them are available using encryption and digital signature.

The first is data integrity. This provides some assurance that the message hasn't been altered. Second, authentication. You would like to make sure that the person you had the transaction with is who they represent themselves to be. The third is nonrepudiation. This is so that an electronic commitment cannot later be denied. Fourth is confidentiality, the privacy of the message. And these four are available using encryption technology and using digital signature.

The fifth, availability, is the assurance that the service will be available on demand, and that requires quite a bit of resource and quite a bit of effort. The analogy is when you pick the phone up you get a dial tone. You can imagine how complex it is to assure that.

So against these benefits you have to counterbalance the potential at least for risks to the users and to society as a whole.

One of the major risks is that encryption can frustrate legally authorized criminal investigations. For example, law enforcement personnel, now with proper legal authorization, are allowed to record telephone conversations when they are investigating suspected lawbreakers. What if these lawbreakers were able to encrypt their communications similar to encrypting financial transactions? They would no longer be understandable, traceable. It is possible

that this could facilitate breaking the law rather than protecting society.

Second, encryption can be a pretty significant hazard for the users. A private firm, for instance, has to worry about the potential misuse of cryptography by their employees. What if there were a rogue employee in a company who encrypted files and then said that they would sell the key back to the management of the company, in effect asking for a ransom? This is usually known as the data hostage issue. You can easily imagine keys being lost or forgotten, and therefore you lose the use of the data.

Because of the risks of strong encryption, the Federal Government is proposing to adopt key escrow cryptography for its own use. This technology allows for the use of extremely strong encryption, but also allows the government when legally authorized to obtain decryption keys that are held by escrow agents, if you will.

On August 17 of this year, the Administration announced its intent to develop a Federal standard for key escrow that would be implementable in software. We already have such a standard in hardware.

As I mentioned earlier, encryption and digital signature can provide very important protections. However, their limitations also need to be recognized. For instance, they are part of a system, and the system has to be managed by people, and the people in the system can be the source of the greatest security risk either through inattention in implementation or indeed maliciously.

Second, the cryptography security measures have to be correctly and securely implemented. Often they are very complex.

Third, the cryptography that you use has to be mathematically sound, has to be strong so that it will resist attack. Also, you need a series of supporting managerial underpinnings. You need a system where the people are trained, where there is physical and intellectual thought put into how to operate the system. This is expensive and not easily achieved, and for a financial management system that covers the entire world, this is a very large undertaking.

Finally, let me summarize by saying that encryption and digital signature technology are likely, in my view, to play an increasingly important role in the protection of electronic financial systems, transactions, and records. Attendant with the benefits of encryption are risks to law enforcement and national security, and, finally, that these risks can be dealt with through a key escrow system.

Thank you, sir.

[The prepared statement of Mr. Raymond G. Kammer can be found on page 131 in the appendix.]

Chairman CASTLE. Thank you.

Mr. Crowell.

STATEMENT OF WILLIAM P. CROWELL, DEPUTY DIRECTOR, NATIONAL SECURITY AGENCY

Mr. CROWELL. Thank you, Mr. Chairman. I appreciate the opportunity to be here.

I am today representing Emmett Paige, the Assistant Secretary of Defense for Command, Control, Communications, and Intel-

ligence in the DOD. He asked that I represent him because we are engaged with ASDC3I and the Defense Information Systems Agency in putting together a large DOD network to serve Department of Defense interests in the future which initially will include messaging services but ultimately may include economic commerce as well. And so we have technical experience in the difficulties in putting together such a large network.

What I intend to do is share with you some of the highlights of my written testimony, which I will not read, which point to some of the difficulties that we will experience in this area.

First of all, we all know that we are developing a growing dependence on our information infrastructure. Networked information systems are being used now to conduct essential business processes, military operations, civil government services, and national and international economic activities.

Earlier it was referenced that there is a decreasing cost in computing, and it is that decreasing cost in computing that is driving the rapid introduction and adoption of such network solutions throughout not only the private sector but also the government and defense sectors as well.

Second, I would like to emphasize what has been mentioned already by several of those who have testified, that security, in the sense of network systems, involves a lot more than just encryption, which is often the subject that is talked about; it also involves other activities that have been described such as data integrity, authenticity, signature, nonrepudiation assurance, and so on, and these are the complete set of services that must be provided in a network environment in order to provide full protection.

What you will find is that in many of the economic areas that have been automated in the past, the most important functions that have been enabled have been data integrity and authenticity, and much less often have the users employed encryption to protect the privacy of the transactions.

Third, I would like to emphasize the increasing vulnerability of information in financial transactions. Information can now be remotely accessed, changed, or destroyed, and I would like to describe how we know that such capabilities are possible.

Defense Information Systems Agency experts recently conducted an attack against 10,000 DOD computers. They gained access to an overwhelming majority of those computers, and only roughly one in a thousand of the successful attacks drew a response from the owners or operators of those systems. So there is, in fact, a demonstrable increased real world vulnerability that DOD systems are experiencing and must protect against.

In 1994 there were 250 unclassified DOD systems—and I emphasize, unclassified DOD systems—that were penetrated, and the attackers in some of those cases stole data, destroyed data, modified software, installed unwanted files, and so forth. There are in every day's press other references to similar break-ins and alterations in the Federal and private sectors in such systems as financial systems, payroll, personnel records, industrial R&D, tax files, credit card records, phone systems, banking, stock exchanges, power distribution, air traffic control, and public safety. In fact,

there is an interesting article in today's *New York Times* regarding the increasing vulnerability of the Internet.

Fourth, I would like to emphasize that DOD recognizes that as it moves into the use of public networks as the principal means of conducting its unclassified business, the DOD will need to provide adequate protection for all of those vital services that are related to conducting DOD business, from mobilization to conducting logistics and support activities of war.

NSA and DISA and ARPA are all working together; NSA providing the information security tools, products, and services; DISA conducting the planning, engineering, implementation, operation and management of the defense messaging system; and ARPA, in cooperation with NSA, doing some advance research in the area of security.

Our key strategic goals are to achieve interoperability so that we can provide for all the DOD agencies to work together, but in fact it is that interoperability that then drives us to provide better security services, because more people will have access.

We will have to have multilevel security so that people with differing needs and differing interests and differing accesses can all use the same system. Otherwise, the cost will be dramatically increased.

We also see the need in doing this DOD job to have a very clear partnership with industry. While we have developed a security system around a card, which I will pull out here, called a Fortezza card, which is a PC card that plugs into a computer, we are doing that with industry, and we are attempting in the long run to make this card compatible with other industry-compatible solutions so we can achieve interoperability with some of the DOD partners, namely the 360,000 people who provide contractual services to DOD and who will want to do that electronically in the future.

Fifth and finally, I would like to mention a challenge that has not been mentioned in detail, but briefly referenced by Ray Kammer. It is a very, very important but little understood problem. Some years ago we created a key management system for DOD's users of the secure telephone unit, the STU-III. It allows for us to certify the users and provide keying services for their encryption. There are about 200,000 users in that network. It was a very expensive undertaking, and it was very challenging technically. The DOD defense messaging system will ultimately be about 2 million users, each of whom will have to be certified and each of whom will have to have their security enabled or disabled depending on whether or not you want them or don't want them to have access. This is a huge management infrastructure that is very costly, and it is one of the fragile and vulnerable aspects of future encryption technology.

When we start imagining providing comparable services for the entire Nation, or for that matter for the entire world, it does indeed look like a daunting challenge at best.

To achieve many of the benefits that the people who have testified have been discussing, such as electronic benefits and distribution of electronic money, will require that that infrastructure be scaled up to a very large size and, in doing so, increase the vulnerability of the system unless it is very, very carefully planned.

That concludes my remarks, Mr. Chairman. Thank you.

[The prepared statement of Mr. William P. Crowell can be found on page 139 in the appendix.]

Chairman CASTLE. Thank you. We look forward to asking you a few questions.

Mr. Diehl, who is the director of the U.S. Mint, is usually worried about whether we are going to endorse the dollar coin or not but is here in a different capacity today.

STATEMENT OF PHILIP DIEHL, DIRECTOR, U.S. MINT

Mr. DIEHL. It is nice to have the opportunity to discuss a topic other than the dollar coin, Mr. Chairman.

I want to thank you for inviting me to testify this morning. As you know, Mr. Chairman, the Mint has taken a strong and active interest in this matter and has begun to work to address certain policy issues related to it. I welcome your interest, the interest of this subcommittee, and the leadership you have shown in calling this series of hearings.

As the subcommittee may be aware, the Mint is participating in the Treasury Department's Electronic Money Task Force headed by the Comptroller of the Currency. The Mint's main interest in the evolution of payment systems is relatively narrow. It is focused on stored-value cards as a potential substitute for coins and currency.

As sole provider of the Nation's coinage, the Mint has an important role in our monetary system. As the use of stored-value cards evolves, many consumers might be expected to replace coinage and currency transactions with e-cash transactions, thus creating a de facto new form of currency. We believe that such a scenario must be studied so the Federal Government will be prepared to address the policy and legal questions that a new form of currency would present.

Mr. Chairman, as I have testified to this subcommittee in the recent past, coins might be considered a declining "second wave" technology of commerce. What we are wrestling with here today are the implications of emerging electronic "third wave" substitutes for coinage and currency. I think we can be informed by a historical analogy that you referred to earlier relating to the evolution of paper currency during the first half of the 19th century.

In the decades preceding the Civil War, to meet the demands of commerce, for which U.S. coinage was inadequate, a multitude of local and State banks issued their own bank notes. As interstate commerce expanded, and private banks failed or merged, the limits of this private system of currency became obvious.

By 1860, the currency market was in chaos and the financial requirements of the war led President Lincoln to preempt the local banks and issue our first national currency in order to facilitate interstate commerce.

Clearly, we do not face the urgency of a national crisis today. However, as you are aware, Mr. Chairman, private parties and a variety of industries are proceeding rapidly to develop their own versions of e-cash systems. It is appropriate to ask the question whether at some point in the future the requirements of market efficiency could accelerate the Federal Government's role in produc-

ing a stored-value card that would augment the use of coinage in commercial transactions.

The issuance of a, if you will, legal tender stored-value card, would also allow the Treasury to retain seigniorage profits that would otherwise be reduced by a decline in the demand for coinage, avoiding the need for additional tax revenue or additional borrowing.

But, Mr. Chairman, questions related to such a significant change in our Nation's currency are not to be taken lightly, they must be carefully studied, and if governmental involvement is deemed appropriate we must define a role that accommodates the emerging e-cash systems of the private sector.

Mr. Chairman, I have attached to my written testimony a copy of the Mint's Reinventing Government II proposal offered as part of Vice President Gore's National Performance Review earlier this year. This proposal was one of seven that the Department of Treasury forwarded to the Vice President.

[A copy of the proposal referred to by Mr. Diehl can be found on page 150 in the appendix.]

In a nutshell, the Mint has proposed that the Treasury Department take the lead in identifying and addressing policy issues related to stored value and smart cards as substitutes for currency, with participation by other Treasury bureaus, the Federal Reserve, other Federal Government agencies and departments, and the private sector.

As electronic forms of payment become more commonplace, reducing the demand for coinage and currency, and in effect becoming a new form of currency, the Federal Government must be prepared to address the policy concerns that will arise.

I look forward to the Mint's continued involvement in this issue, and I look forward to continuing to work with you in those efforts.

Thank you.

[The prepared statement of Mr. Philip Diehl can be found on page 146 in the appendix.]

Chairman CASTLE. Thank you, Mr. Diehl. I know you have been involved in this issue for some time. We appreciate your abiding interest in this.

And finally we will hear from Mr. Robert Rasor, who is the deputy assistant director for investigation for the Secret Service.

STATEMENT OF ROBERT RASOR, DEPUTY ASSISTANT DIRECTOR FOR INVESTIGATION, SECRET SERVICE

Mr. RASOR. Thank you, Mr. Chairman, for the opportunity to address this subcommittee today—and I will quote—on the subject of the future of money, the future of payment systems in the United States and abroad, and the public policy implications of the technologies involved. Extremely long title.

We have submitted a rather in-depth statement for the record, which is unusual for us, but we found this area to be of great interest to us and great importance, so we submit the entire statement for the record.

My comments today will really kind of center around some of the comments that you made in your opening remarks, which were of significant interest to us, and that is the private sector agreement

and the systemic threats and the ability to blend those things together, and perhaps even touch on Congressman Metcalf's comments on who really creates the money in the country and what happens to it from that point forward.

I have with me today Mr. Mike Stenger, who is the special agent in charge of our Financial Crimes Division, and Mr. Bob Friehl, who is from our Electronic Crimes Branch, who helped in the preparation of the testimony.

The Secret Service is uniquely qualified to discuss with you today the past, present, and future of money and the monetary transactions in both the domestic and transnational sense. The jurisdiction and responsibility to detect and investigate Federal interest crimes in the credit card access to vice electronic payment systems was conferred upon the U.S. Secret Service by Congress with the passage of the 1984 Comprehensive Crime Control Act.

During the past decade, the U.S. Secret Service has dedicated countless investigative hours to control the counterfeiting and other fraudulent payment schemes developed to exploit the systems. Just as important, however, though, is the risk analysis process and the developed understanding that the Secret Service has acquired in relation to electronic crimes and the techno-criminal.

Proceeding with a working definition of electronic cash as being financial compensation, exchange or transference through electronic media, the Secret Service has established rapport with many of the industries that will be cultivating, developing, and/or facilitating this activity.

The telecommunications industry, wire-line and wireless, is really the backbone upon which much of this industry is being developed. This agency has worked with these carriers and manufacturers for years to identify and address vulnerabilities inherent to the development of the respective systems and clientele.

We have also been associated with the credit card industry and financial institutions as they have evolved through their marketing and technological expansions. We worked with them during the development of telecards, smart cards, biometric authentication, and interactive opportunities, and most recently as they maneuvered to meet the demands for electronic compensation. Historically, these industries in our economy have been exposed to millions, if not billions, of dollars in fraud and related exploitations.

Our commitment has contributed to the recognition and adoption of positive solutions to systemic problems. The result is a product which is more fraud resistant yet viable in the marketplace. Through our proactive risk analysis process, we have come to understand the systems and particularly the weakness of the systems that are exploited by the criminal community. It is with this collective institutional understanding that I will today make a couple of comments and some recommendations.

Circa 1865, the payment systems became the national currency, due in part to the fact that roughly one-third of the currency in circulation in the United States at that time was counterfeit. The Secret Service was originally created to combat the counterfeit problem, an issue that had threatened the country's financial systems.

In the early 1980's, credit cards and other emerging types of access device payments were targeted and compromised by organized

criminal elements. Although we continued to utilize technology to limit the effects of fraud, the criminals also used enhanced technology. We have learned valuable lessons in law enforcement in the value of law enforcement establishing partnerships with business and industry.

The lesson of the past is basic: Create the partnership before the systems are put in place. A good example of this process is the electronic benefits, or EBT, task force concept, in which the government is taking the time to appropriately design the system before it is employed. Congress may act as a mediator in this process by requiring that the proposed cyber systems show a demonstrated ability to protect themselves and assist law enforcement when direct or indirect abuse occurs.

A recommended approach for those responsible for the management and marketing of the systems is to specifically define what the Service is going to provide. This will enable law enforcement to outline the potential criminal abuses in these services and recommend fixes prior to problems.

Experience has shown that past, present, and future criminal activity is evolutionary in nature, and the lessons learned may serve to prevent reoccurring and future problems.

A second recommendation focuses on the need for law enforcement and the industry to establish and maintain active working relationships. For this effort to be productive, it must be deliberate and continuing rather than cyclic. The relationship must facilitate the exchange of information and technology.

Technical evolution has no startup nor completion date. By definition, it is ongoing. Having recommended that the cyber industry should be held accountable and that partnerships be promoted, we would also proffer that Congress should remain engaged in this process.

The Honorable Bill Nelson, cosponsor of the Computer Crime Bill in 1984 said, quote: "Where people work daily with a powerful tool such as a computer, there will be those who step over the boundaries between legitimate and criminal uses of these high technological devices." Currently technology has outgrown the regulations. The laws within this country have to address these new issues before we can ask other countries to do as we say and not as we do.

There can be safe alternatives to currency exchange on the Internet and also offline. Combining the lessons learned to date, implementing existing safeguards, and creating future agreements in the international arena will guarantee that secure alternatives are pursued.

Education, the spread of knowledge, and the increase in necessary law enforcement resources will help protect the United States against Internet attacks. The objectives should be to understand and control electronic monetary risk and vulnerabilities, thus providing and promoting confidence to the global electronic marketplace of consumers, investors, taxpayers, and the public.

The Secret Service has a decade of hands-on experience with electronic cash and 125 years of experience in currency protection. There is overwhelming evidence to indicate that technological enhanced payment systems are a reality which will grow in large pro-

portions. If the opportunity for the inclusion of comprehensive security measures lapses, the direct and indirect costs associated with retrofitting the technology would be devastating.

That concludes my remarks for this morning. If you have any questions, I would be happy to answer them.

[The prepared statement of Mr. Robert Rasor can be found on page 160 of the appendix.]

Chairman CASTLE. Thank you, Mr. Rasor.

Let me start with Mr. Diehl. I want to shift to some security questions from there.

You mention in your testimony that currency and coinage could be replaced by e-mail or could be replaced by electronic mail or whatever it may be, electronic devices. What about the whole currency issue and the whole seigniorage issue, which is a matter of some concern to us?

We are always interested in making money on these things and helping out with our debt problems. At some point do you fear that that becomes an issue in all this? Initially, of course, it won't be that much, but what happens 15 or 20 years from now?

Mr. DIEHL. I think that is probably—certainly from our perspective at the U.S. Mint—the threshold issue. We are concerned about, under a scenario in which there is rapid expansion of the use of e-cash devices as a substitute for coinage and currency, that we would see a significant reduction in the demand for coinage and for currency and a loss of seigniorage profits that goes to the Federal Treasury, and the U.S. Mint alone produced \$700 million in seigniorage profits last year. That was near the peak of what we have done over the last 10 or 20 years.

And of course there are also profits from the Bureau of Engraving and Printing's production of currency, that while it immediately goes into the accounts of the Federal Reserve Bank, it nevertheless does eventually find its way into the General Fund.

So there are substantial revenues at risk if this technology, emerging technology, really takes off.

Chairman CASTLE. I think it is something we are going to have to keep our eye on. I hadn't thought about it a lot, but it is clearly a factor.

Maybe to the others, one thing that—or Mr. Diehl is welcome to try to answer this, too. We had a little session in New York City and had about 40 people there and discussed some of this, and one of the issues that was raised there is the whole issue of privacy.

You have touched on the security issues, and I guess it is relatively easy to do security, but in doing so, you are asking individuals to give up their privacy, and that is something which some people abhor and, frankly, are going to resist in any way possible.

So you have a situation in which it is going to be very difficult to regulate if you are going to recognize the individual's right not to have any of their privacy disturbed.

How do you balance these two items? How do you deal with that, to me, almost irreconcilable conflict to some degree?

Mr. KAMMER. Sir, if I could comment, I don't think there is a completely satisfactory way to deal with this. The greater the assurance of privacy, the greater also the potential for abuse of that

assurance in breaking of the law and in damaging society in some large or small way.

And the balance point sought before encryption was thought to be possibly widely diffused in our society was that in order for law enforcement to look into someone's communications, they had to persuade a judge, they had to pass some pretty hard tests, and indeed, the current state of the debate, at least for the Federal Government, is the thought that we would maintain that balance at that point and that, in the absence of some compelling argument that there was a law being broken that would persuade a judge, that people's assurance of privacy would be as good as the quality of the encryption they used.

If it were persuasive that the law were being broken, or at least were possibly being broken, then the government would be able to draw a key that had been escrowed and at that point be able to solve, if you will, the encryption.

The number of times that the government actually goes in and uses this authority is very small. I think in most years, for the entire government, it averages around a thousand, both State and local and Federal.

Chairman CASTLE. But this could change.

Mr. KAMMER. It certainly could.

Chairman CASTLE. I mean as you get in a situation in which people are intentionally concealing transactions and monetary movement, I would think it could change dramatically.

Mr. KAMMER. When the payoffs get large, it will draw more criminals.

The potential for transferring large amounts of money anonymously is an extremely attractive one, as was described by a number of witnesses earlier. That not only draws more people but maybe more sophisticated people, and the potential damage to society gets larger.

Chairman CASTLE. Did you want to comment on that?

Mr. RASOR. Well, I would just follow up by saying that I mean the issue of privacy becoming more of a factor in a future system is really relative to where it sits right now. I think that question was just now responded to.

There are safeguards, and there are provisions now that allow for access to a system, be it a paper system or a semi-cyber system that currently exists. I think that those safeguards and those regulations or laws, upgraded to define the new cyber systems, are appropriate and needed, and I think fairly widely accepted, as a law enforcement tool.

Chairman CASTLE. I am going to turn to Mr. Metcalf, but I might suggest just as sort of a political warning or lightning rod, if you will, that that is an issue of some vital concern to many people out there. I think it is one that needs to be carefully thought out in terms of providing the protection, but at the same time not endangering privacy in any way.

It is a heck of a lot different from subpoenaing a bank record or something in writing that you normally would not have access to, because I think people generally believe that, when you get on the electronic networks, that, plugged in correctly, the government could get access, and I just think it is going to make some of these

future transactions very difficult if that question is not well thought out and well articulated in terms of the public understanding exactly what their rights are versus whatever the public rights are to the protections which might be needed.

Mr. Metcalf.

Mr. METCALF. Thank you, Mr. Chairman.

Sort of back to this—I keep trying to go around on this issue, so I will ask it sort of again. Let's assume that it is very necessary that the Fed retain real accurate control of the Nation's money supply. Now whether or not that is true is another question, but let's assume that it is.

Might it be necessary to enact legislation to somehow be sure that the Fed knows that the electronic money that is out there all correlates to the money that the Fed has issued, or isn't it important?

Where you are monetizing, essentially monetizing credit—not you, but these cards are monetizing credit—is this related? Is this important? Part of me says yes, you have got to have some sort of control of the money supply. The other side says, well, why? Do you really have to? This is a different kind of thing. So any comments on this?

I am really puzzling over this question. Basically how will the Fed know that the electronic money out there is money that they have issued instead of new money that is being created and added to the system?

Mr. RASOR. Well, if I could pick up on this question just a little bit, I mean that touches on an issue of Federal interest in reality, and once you start imagining how a system changes from a green-back to a burst of energy developing commerce, I think really two things come into control or interest there, and it may come to pass at some point that if you go computer to computer and you use what they are currently defining as cyber coins, where something is developed you put in your computer and you get on the Internet, you see a shirt that you want, you send one of your coins down the road, the shirt comes back to you eventually, perhaps those sort of activities and losses resulting from those activities may not be a Federal interest, because no financial institution is involved, no funds are insured.

It would be synonymous with you losing cash on a street corner as opposed to losing cash through somebody going into your bank account and taking money out of it.

I think where that is going to kind of even out in the marketplace is when and if somebody gets victimized along that line, and that becomes publicized and the vulnerabilities are realized and there are no recovery mechanisms built into that process, it may take some thought process on the public: Do they really want to get involved in that system?

But on the other side of that, the other Federal interest of course is the tracking. You know, the tracking is an interest, all the way through, where the Federal Government has an interest in knowing where the money is going, how it is being utilized, whether appropriate taxes are being paid, things of that nature.

Mr. METCALF. I was thinking of another issue really, the—you know, as I have watched from a far distance of Washington State,

watched things work, it was assumed that the money supply related to inflation, and if the money supply got too high, inflation took place. Well, now there is another interest. That is the one I was really thinking about.

If we see the money supply expand dramatically sometimes and inflation didn't happen, what was the difference there?

And I shouldn't be asking you, I should have asked Mr. Blinder that question, I am sure. But at least that is the kind of thing I am thinking of, not so much the government tracking but the relationship of the money supply to inflation, and if that is really true, and we assume it is, then a vast expansion via this system could have impacts that we aren't really watching for.

If you have any comments on this, I would appreciate hearing them. I do realize it is a little out of the scope of the people sitting right here.

Chairman CASTLE. I am going to—I would like to just ask a couple of questions of Mr. Diehl, if I may, which were in my notes here which, I think are at least interesting, and we will try to wrap it up.

I know it is running a little bit late here.

Under what circumstances should the U.S. Government enter the market for e-cash instruments such as stored-value cards, and why shouldn't this market be left to private sector providers entirely?

Mr. DIEHL. I think the first topic that we talked about, the potential loss of seigniorage profits, is the one that is most obvious, the most obvious Federal interest that we focus on. But I am not certain whether that interest is sufficient—and certainly it is probably a longer-term interest—to justify Federal entry into the market.

I think there are probably other policy objectives that are going to be more important to determining whether or not the Federal Government has enough of an interest to get into the market for stored value cards. A number of these issues we have talked about this morning; for example, whether or not Federal entry into the market could make a substantial contribution to system efficiency or whether it would increase public confidence in this particular type of instrument.

Also, I think Federal entry into this market might make a major contribution in the accessibility or the affordability of this technology, some of the issues that we heard about earlier this morning—concerns about service in low-income markets. If, for example, there are substantial charges proposed or imposed by the private sector on the use of these cards, there may be a Federal interest in participating to ensure that the cards are available at face value.

So I think these are the kinds of larger policy issues that are more likely to arise before we really see the threat to seigniorage emerge as a significant factor in the question.

Chairman CASTLE. Here is my favorite question. It is sort of a follow-up to that, and this provokes other thoughts on what the private sector could do as well. But is there an opportunity for the Mint to produce collectible versions of stored-value cards and thereby generate additional revenue for the U.S. Treasury?

We are always looking for ways to get a little extra revenue, get taxes down, whatever it may be. You know, I can think of all kinds of cards that might be of interest out there.

Mr. DIEHL. Well, there is no question there is a market. This is something that we have seen because we are active around the world in the selling of our U.S. Olympic Commemorative Coin series right now, and we have seen an extraordinarily strong market for collectible versions of these stored-value cards. It has been late coming to the United States. It has been a very active market in the Far East—and now in Europe—for the last several years.

So I think there is no doubt that there is a market there. How big it is, I don't know. I think it is certainly in the tens of millions a year in terms of revenues, and perhaps that much in terms of profits.

Of course, as you know, Mr. Chairman, we are concerned about the proliferation of commemoratives in the coin market, and this is something that we have had numerous conversations with you about, and I think our interest in the potential for issuing commemorative stored-value cards would be colored by the additional complications or the ability to uncomplicate our situation in the commemorative coin market, so that we get a better handle on that market as well.

Chairman CASTLE. Well, we are working on the commemorative coin issue, as you well know, with you and hopefully will have some resolution of that. Certainly we don't want to issue commemorative coins on which the government does not break even. Let's make some sort of a profit.

Let me thank all of you, and as Mr. Metcalf leaves, let me particularly thank him for staying with us throughout this. He really is an expert on a number of these issues. You have been very kind to be here and to give your time.

I think what we have discussed today is of vital significance to the commerce of the United States of America, and indeed the world, in which these commerces might blend, I might add, over the course of time. Our responsibility, I think, is to gather this information and to store it correctly, and as we need to do something with respect to regulations, we will start to look at them. Again, we would have hearings, but we are not leaning in that direction at this time.

I wish you would feel comfortable in giving whatever input you have to our subcommittee at any time. You don't have to wait for a formal hearing.

As I mentioned to the first panel—and you were in the room—we may wish to submit additional questions to you. We don't have time at these hearings to often ask all the questions we would like to.

Finally, I would like to mention John Lopez, who is the staff assistant for this particular Subcommittee on Domestic and International Monetary Policy. And if anyone in the audience here today or watching on television wishes to add input to this, because I know a lot of you have ideas, I wish you would feel very comfortable in sending that to Mr. Lopez, care of the House Banking Committee in the Rayburn Building in Washington, DC., because we are interested in learning all that we can. This is a quest for

information, and you may have heard something which you agree or disagree or know something different, and we would be very interested in knowing that as well.

We can't, unfortunately, get this room to have hearings every day, nor do we have time to have hearings every day, but we are interested in gathering as much information as we possibly can. I think this has been very fruitful, very worthwhile. It is the building block on which hopefully we will make correct policy decisions in the future, and I think if we continue to talk to each other we are much more likely to make those correct policy decisions. So it served that purpose.

Again, I thank you, and, with that, we stand adjourned.

[Whereupon, at 12:40 p.m., the hearing was adjourned.]

APPENDIX

October 11, 1995

(41)

PREPARED STATEMENT OF CHAIRMAN MICHAEL CASTLE

The Future of Money Hearing - October 11, 1995, 10:00 a.m.

Room 2128 Rayburn House Office Building

Follow up to the July 1995 hearing to explore the impact of new technology on future payment systems, money supply, privacy issues, security and regulatory compliance issues with public sector witnesses.

Chairman's Introduction:

The subcommittee will come to order. Welcome to the House Banking and Financial Services Committee, Subcommittee on Domestic and International Monetary Policy Second Hearing on the Future of Money. This Subcommittee bravely continues to go where no one has gone before, although it is within the scope of our jurisdiction over important areas of public policy.

The Future of Money, that is to say the shape and character of the future media of exchange via electronic commerce, may well form the underpinnings of the next great expansion of world-wide commerce. This intersection of technology and commerce has been predicted to fall at almost every point along a continuum ranging from "over-hyped fad" to "change with implications as profound as the Industrial Revolution". As we noted in our July hearing on the subject, whether it occurs over computers linked into networks or via computer chips embedded in cards or other devices, the potential exists both for great commercial promise and for considerable risk of undermining currencies, systems of exchange and the administration of justice.

It is incumbent on Congress and Executive Branch Agencies, including law enforcement, to try to understand these technological innovations and the implications they hold for our future. For this reason, we have initiated this series of hearings. It will not end with the session today. At least one more is in order. There, I hope we can bring together representatives from banking, consumer groups, legal experts and technology companies not yet heard from. The aim would be to initiate a process of consultation leading ultimately to private sector agreements that would address the key public policy questions that will be discussed today. I believe that most of my colleagues on this subcommittee, would share my preference to see Internet compacts and international industry agreements attempt to neutralize systemic threats. At least a genuine effort should be undertaken before turning to sovereign states to attempt the management of cyberspace. You may be very certain that if this challenge is beyond the reach of the private sector, there will arise an irresistible pressure for government or some supranational authority to police this new world. This kind of official reaction can be expected only to stunt the development of commerce, art, and other creative exchange across these electronic links. The Financial Crimes Enforcement Network, shares these concerns, they already have the responsibility of applying the Bank Secrecy Act in the countering of money laundering. They held a valuable Cyberpayments Colloquium two weeks ago in New York City and the organization produced a useful working paper that is included in condensed form in each member's folder. We are pleased

that Stan Morris the FinCEN Director has been able to make it back from China in time for the hearing today.

At our last hearing, we quoted Philip Diehl, Director of the Mint, who will appear before the subcommittee today and tell us about the Mint's vision of electronic currency. He has compared the current status of Electronic forms of money to the situation before the Civil War when local banks issued their own paper money. He foresaw that left alone and unregulated, the market might produce an electronic "Tower of Babel", with no technology standardization and many opportunities for law avoidance and criminal transactions. We are gathered to continue our exploration of these emerging "Third Wave" forms of currency and hear more about the appropriate role of the federal government.

This morning, we will hear from eight expert witnesses, drawn from the federal government. With their assistance we can begin to consider some of these vital issues. For convenience we have divided the group into two panels. The first has primary expertise to address aspects of the integrity of the monetary system and the second will no doubt discuss issues of privacy, both commercial and personal. Both groups are free to overlap on issues and take the discussion where their particular institutional expertise leads them. In short, we will consider in greater depth, public policy issues raised at the first hearing.

Cooperative efforts between banks as an industry and between banks and the government have made current payment instruments successful and widely used, and if analogues to these precedents can be found for future payment mechanisms, they may be made similarly successful.

We are fortunate to have before us eight eminent public servants who have charged with great responsibilities in the managing of our national economic security, law enforcement, sound money and communications security.

They are:

Alan Blinder, Vice Chairman, Board of Governors of the Federal Reserve System

Eugene A. Ludwig, Comptroller of the Currency.

Stanley Morris, Director, Financial Crimes Enforcement Network.

Sally Katzen, Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget.

Raymond Kammer, Deputy Director, National Institute of Standards and Technology.

William P. Crowell, Deputy Director, National Security Agency.

Philip Diehl, Director of the United States Mint.

Robert Rasor, Deputy Assistant Director for Investigation, Secret Service.

STATEMENT OF FLOYD H. FLAKE
RANKING MEMBER
SUBCOMMITTEE ON DOMESTIC AND INTERNATIONAL MONETARY POLICY
OCTOBER 11, 1995

THE FUTURE OF MONEY: PART II

Electronic banking and its ramifications on not only the national but global economy are real issues of importance to the Banking Committee, its members and our constituents. This statement will outline some of the current technology that facilitates electronic banking and commerce, and also some of the security and regulatory problems these new technologies might pose.

Stored Value Cards

According to Visa, bank cards are now the third most important means of consumer payment after cash and checks. Annually, they account for about \$1 trillion of purchases worldwide, \$463.1 billion of which are in the United States. Corporations, like Visa and Mobil, are introducing Stored Value Cards, hoping that this new technology will be the successor of the ATM card. These cards have more appeal because banks estimate that four percent of the value of deposited cash is eaten up in handling costs.

A stored value card will operate like an electronic "purse" or "wallet" that will take the place of coins and cash for small purchases. These will be wallet-size cards embedded with rechargeable microchips in which the consumer will be able to "reload" the micro-chip and control the amount of value stored in the card's memory. As opposed to the pre-paid phone cards that are currently popular here and in places as far away as Malaysia, the value information is stored in the card and not in a central computer repository miles away. One of the most extensive deployments of the technology so far has been in Denmark, where a consortium of banks and telephone companies, known as Damont, has issued more than 150,000 stored value cards, aimed at very small transactions such as those at parking meters and soda machines. One of the most popular applications has been in laundromats, which have found that the cards reduce theft and vandalism due to the absence of coins in the machines.

Visa and its members plan to showcase their chip-based prepaid card application during the 1996 Summer Olympics at Atlanta. Meanwhile Key Federal Savings Bank and Mobil Oil Corp have introduced a stored value card for purchasing gasoline and other services. Unveiled in Dallas, this service allows consumers to load up their card in denominations of \$25, \$50 and \$100. This is a precursor to the technology that Visa and others have introduced, though, since it operates on a magnetic stripe and on-line connections, and not on an integrated circuit chip. On the other hand, First of America Bank Corp. Will install the first bank-issued smart card university system at the University of Michigan and Western Michigan University this fall. This smart card will function as an identification card, an ATM card, a stored value card and a building access card. More than 200 merchants near the campus are expected to accept the card. Other

companies hope to develop cards that will house reservoirs of information for the consumer. These include information on the holder's credit lines, finances, car registration, passport, medical records, door key, and notes and reminders.

Concerns

The stored value card will definitely be a plus to consumers, especially as the technology advances. There are, however, some concerns that go along with the benefits of these new ideas.

- Will stored value cards keep financial transactions anonymous?

Presently, with cash, once a transaction is complete it is virtually impossible to trace who made the purchase. Many Americans value this anonymity when conducting business. This technology has the possibility of tracking people and keeping complete records of their purchases. This is a plus when it comes to surfacing the underground criminal economies, but can definitely encroach on the privacy of law abiding citizens.

- How secure can a stored value card be?

The current technology being developed calls for a microchip that can be read and written. One concern is, using the University of Michigan smart card system as an example, what if someone sets up a dummy door access machine that can actually read information off of students' smart cards. This person would then be privy to other students' ATM and stored value cash. Unlike cash, integrated chips are subject to damage which could alter one's value of money available. A torn or wet bill is relatively easy to exchange for the same value, but what about a worn or bent stored value card?

- How will this technology affect poor communities?

If this technology is a successor of the ATM card and there are very few ATM machines in poor neighborhoods, where does this leave them? Many see the electronic purse as eliminating cash, so this could have a severe effect on neighborhoods that are currently under served by financial institutions. The implementation of this technology would seem to take effect in these neighborhoods last, and dampen the ease in which their citizens can perform necessary daily purchasing tasks.

Electronic Banking

Electronic Banking is taking place every day. From ATM transactions to simple credit card purchases, currency is being exchanged over phone lines. The future, though, bodes well for all banking functions being performed over the Internet and even the complete elimination of cash.

In the near future consumers are going to be able to make payments from touch tone phones, personal computers, screen phones, personal computers and personal intelligent communicators. This technology will then lead to "virtual banking", so consumers will be able to

make deposits, pay bills, invest in stock, purchase an insurance policy and take out a mortgage loan without ever actually seeing their banker face-to-face. There are many companies that offer some sort of on-line banking services that can be accessed by doing a Net Search for electronic banking.

Concerns

There is no question that electronic banking offers convenience and the safety of banking at home, but there are also concerns that arise.

- How secure are banking transactions that occur on-line?

As with any transaction that occurs over the phone lines, the issue of security is a big concern. There are forward thinking companies, such as Electronic Data Systems (EDS) and Cybercash, which handles credit card payments, which have created encryption systems to secure financial transactions over the Internet. Electronic Data Systems takes customers off the Internet and places them onto EDS' private network, where all transactions are secured with encryption. As with the stored value cards, will some hacker be able to copy the digital codes that the funds are being transmitted on (like cellular phone "cloning")? Digital forgeries are also a real problem, since they are by definition, perfect copies (two identical strings of numbers).

- How will people recognize a legitimate on-line bank?

With more than 30 million users today and 200 million projected to come onboard in the next two years, there are a vast number of people who could use the Internet for ill gains. Any organization can become a global publisher by establishing an information site on the Internet's World Wide Web. Thus, criminals could possibly download vital credit card and stored value account numbers by setting up their own home page.

- How will the government be able to regulate commerce and banking on the Internet?

Some "cyberpunks" have suggested that the ultimate e-cash will be a currency without a country, with maybe corporations like Visa and MasterCard controlling the currency. In the November 26, 1994 edition of The Economist, an article titled "So Much For the Cashless Society. (Electronic Money)" the author raises some very interesting points.

"If people who log on to the Internet are localized geographically and thus subject to a particular set of national laws, the traffic that they create on the Internet is not very obviously anywhere at all. When global digital cash becomes a reality, tax men will have their work cut out deciding how to assess assets that might be stored on a different computer in a different country every day, even assuming they could ever find the assets or the computers. And for those who chose to evade tax actively, the opportunities offered by the Internet would be absurdly tempting, just as they already are for pornographers."

Another school of thought on this subject suggests that “Money does not have to be created legal tender by government: like law, language and morals it can emerge spontaneously. Such private money has often been preferred to government money, but government has usually suppressed it. (F.A. Hayek, **Denationalisation of Money - The Argument Refined**) ”

Finally the issue of keeping up with the constantly changing technology is one that the government has to keep a keen eye on. Will developers be able to create new technologies that will make loopholes in the tax law, faster than agencies can re-regulate, etc.?

- How will electronic banking affect poor communities?

As noted above in the stored value card section, poor communities lack neighborhood banking services. An absence of these institutions and the money to help provide the new technology to these communities, will help deepen the economic turmoil that rural and urban communities of America are already in. The elimination of cash as legal tender without fully supplying every American with the opportunity to interface with the new technologies, could set a dangerous precedent in further limiting the ability of these communities to revitalize themselves economically.

For Release:
10 a.m., October 11, 1995

TESTIMONY OF
EUGENE A. LUDWIG
COMPTROLLER OF THE CURRENCY
Before the
SUBCOMMITTEE ON DOMESTIC AND INTERNATIONAL
MONETARY POLICY
of the
COMMITTEE ON BANKING AND FINANCIAL SERVICES
of the
U. S. HOUSE OF REPRESENTATIVES
October 11, 1995

Statement required by 12 U.S.C. § 250:

The views expressed herein are those of the Office of the Comptroller of the Currency and do not necessarily represent the views of the President.

Mr. Chairman and members of the Subcommittee, I welcome this opportunity to discuss recent developments in electronic money and payment systems and the issues they raise. As supervisor of national banks, the Office of the Comptroller of the Currency (OCC) has a keen interest in the future of money and payment systems, both in the United States and abroad. My appearance at today's hearing is in keeping with the long history of our agency. Congress created the OCC in 1863 to oversee the establishment of a uniform national currency. Today, the OCC is committed to helping maintain a banking system that will meet the needs of the vibrant, diverse, service-based economy that will ensure the prosperity of our Nation. In addition, Secretary Rubin has asked me to serve as the Treasury Department's coordinator on electronic money issues. From both perspectives, I am convinced that steps the government takes--and perhaps, equally importantly, does not take--will fundamentally influence the direction of the future of electronic money and the payments system in our economy.

The development of electronic money clearly gives rise to important and legitimate areas of government concern. Because the electronic payments area is rapidly developing, it is incumbent upon government to follow those developments carefully to ensure that the public interest is served. At the same time, government must be ever mindful not to unnecessarily impede free market developments.

To glimpse into the future, we can look at recent developments in payments technology. These developments will continue, increasing the quality and reducing the costs of retail payment vehicles. Although the benefits to consumers and businesses are potentially great, the technological and policy issues associated with some of these payments vehicles trouble many observers in both the public and private sectors. In my testimony, I will discuss some potentially important developments, identify the major concerns, and attempt to place those concerns in the context of the ongoing evolution of payments mechanisms. I will also offer some preliminary observations on the appropriate role of government in the development of electronic payments systems.

Recent Developments

The convergence of recent advances in technology and changing consumer demand are broadening the array of payment options available to consumers. One such development is electronic banking, which allows consumers to use their touch-tone telephones, home computers or debit cards at retail establishments to authorize their banks or other third parties to issue payments drawn on their bank accounts, or to engage in other banking activity.

A second development is electronic cash, which, unlike electronic banking, represents an alternate medium of exchange. A firm, which may not be a bank, issues claims that are accepted as payment, and, acting as a clearing house, redeems the payments. One manifestation of electronic cash is the smart card, a stored value card with an embedded computer chip that some are marketing as an electronic alternative to cash. As my statement will discuss, electronic cash raises a host of important new policy and regulatory issues, including questions of who should be permitted to issue this new form of money and what, if any, changes in the legal and regulatory structure are appropriate.

Analysis of those issues is complicated by the many different shapes that electronic cash systems can take. Electronic cash can be stored directly on a smart card or on a central computer that is accessed with the card. It may be issued and redeemed by a single entity or by multiple entities through a central clearing system. There are closed-system smart cards that are accepted by a limited set of vendors, which have gained popularity on college campuses and with mass transit systems, and open-system cards, yet to come to market, that would be universally accepted as cash equivalents by multiple vendors. Eventually, these electronic cash systems could be a vehicle for the exchange of other, non-financial information. In this case, the regulatory response must recognize and accommodate a potentially new, larger connection between banking services and the capture and manipulation of information.

A related development, often referred to as electronic commerce, allows purchasers to conduct remote transactions electronically, using the telecommunications network. For example, consumers can browse the Internet to select merchandise from on-line catalogues and pay by providing a credit card account number. As currently conducted, electronic commerce on the Internet uses the existing payments system. In the future, however, consumers may be able to make purchases by transmitting funds directly over the Internet.

As we consider changes in the payments system, it is useful to consider why some product innovations are successful and why some are not. In a market system, successful innovations gain consumer acceptance because they add value by solving problems. The automobile is one such innovation. One of the most influential product developments in the last century, the automobile developed rapidly in the United States largely because it helped people overcome the vast expanses of the North American continent. Unlike Europeans, who enjoyed comparable economic means but who lived closer together, Americans bought cars for personal transportation and so they could socialize with each another.

One can think about current innovations in money and payment systems in the same way. These innovations will develop rapidly if they solve problems in the particular environment in which they are used. Precious metals were one of the first widely accepted exchange media, because they are somewhat portable, durable, and easily recognized. Those metals were later minted into coins, making their value more easily discernible. A subsequent innovation was payments through bank transfers of one kind or another, which provided a convenient, more reliable, and safer substitute to coins. Paper currency emerged as another replacement for coins because it is more portable, and hence more convenient, and while it is less durable than coins, it is cheaper to produce. Eventually, checks largely replaced currency in many transactions because they offer, in addition to increased convenience and divisibility, proof of payment and some security. To a great extent, wire transfers over telephone networks have displaced paper checks for larger transactions because they offer a more convenient, secure way to conduct remote transactions. Credit cards, a relatively recent addition to the array of retail payment vehicles, have gained wide acceptance because they enable consumers to conduct remote and face-to-face transactions in a more secure and convenient way.

We expect more innovations in means of payments that fulfill the fundamental economic roles of money in new ways, but consumers will ultimately decide whether these innovations succeed. Smart cards, for example, may well gain acceptance as a means of exchange if they can extend the convenience and security advantages of other bank cards to lower denomination transactions typically conducted with paper currency or coins. Electronic commerce over networks may prove superior to telephone-originated mail order retail purchases if it extends the advantages of remote commerce to a wider array of transactions, or makes it easier to conduct.

Notwithstanding the promised benefits, current developments in electronic banking have raised concerns about the adequacy of government oversight in the face of anticipated dramatic changes in the business of commercial banking. For some market participants, the changes are desirable because they signal dramatic opportunities. For others, however, the mere association of sophisticated advances in computers and telecommunication technology with banking is alarming. Electronic banking may seem dangerous because the money is intangible and because the parties involved in the transaction may not meet or even speak to each other. Furthermore, some of the avenues through which electronic commerce might be transacted lie outside of the banking system, which has been a source of confidence for consumers. Finally, a significant number of consumers may not be able to afford the devices that are currently being proposed as avenues of access to electronic banking systems, and hence they fear exclusion from what could emerge as one of the primary means of payment in our economy.

Worries about electronic payments have led some to call for government intervention in areas such as monitoring of electronic commerce, requiring a role for banks in the conduct of electronic commerce, and the establishment of standards for security and the protection of customer privacy. Also, the government could become a major issuer of electronic money. Before I discuss the specific concerns associated with the development of electronic money, I think it is important for me to offer a framework that will help put these concerns into perspective.

Government's Role in Responding to the Changes

As we consider the role of bank supervisors and other regulators with respect to electronic cash and payments, we need to first remind ourselves that these developments are only the latest phase in an evolutionary process that began centuries ago. The development of a nationwide communications network was the first phase in the evolution of electronic payments. On this network of telephone cables, businesses and individuals eventually were able to use wire transfers to move large sums of money more quickly and securely than in any previous payments system.

The mid-twentieth century marked the beginning of the second phase in the evolution of electronic payments, the computer era. Advances in computer technology provided the means for processing large volumes of small payments at low cost, supporting first the automation of the traditional check payment system, using magnetic ink character recognition technology, and later the development of the credit card industry. That industry used magnetic stripe technology, and its limited capacity for storing information, to create cards that were portable and durable.

In the current phase, many banks have introduced, or are planning to introduce, remote full-service banking. Recent advances in telecommunications and computing capacity may enable banks to provide electronic access to most banking services through telephone, cable television, and personal computer links. These technologies could extend home banking to most and perhaps all of the services that up to now have been accessible only in a branch office, including the ability to make electronic payments, receive funds and make deposits, and to the conduct of electronic commerce and banking over the Internet.

The advance of technology has, however, been uneven. Smart card technologies gained significant footholds in France in the 1980s, but are only now being considered as a serious payments alternative in the U.S. Meanwhile, the use of credit cards and other magnetic stripe technologies, which has gained wide acceptance in the U.S., is much less prevalent elsewhere in the world. Moreover, some anticipated changes have been very slow in unfolding. Despite predictions to the contrary, Americans still write many checks, and home banking by phone has had a history of starts and stops.

We can draw several lessons from the evolution of payments and communications technology. Change is inevitable, although not always rapid or predictable. While government needs to adapt to change, that adaptation should itself recognize the possibility of further change. And while government should try to anticipate problems that may arise from future changes, it cannot rely too heavily on predictions. Equally important, some of these changes may not pose new problems and therefore may not require any change in government's role.

Nonetheless, there have been and will continue to be some issues related to electronic payments that government should address. Drawing on the Administration's work on reinventing government, we have distilled four guiding principles to direct the appropriate government response:

First, government should only intervene when there is a clear need to advance the public interest. In responding to the challenges posed by new technology, it is government's role to protect the public interest, ensure the efficiency and competitiveness of our markets, and maintain public confidence in our financial institutions and payments system.

On some occasions, government has been able to make the market process more efficient with minimal intervention. For example, by establishing a standard rail width, government facilitated the building of the intercontinental railroad in the 19th century. Government involvement in U.S. securities markets to ensure fairness has maintained investor confidence and helped facilitate financial stability. Similarly, it may be appropriate at some point in the future for government to set standards that apply to electronic payments vehicles. For example, government may have a role in setting and monitoring standards to address security issues, or it might participate in the establishment of new standards to discourage fraud and abuse. Certainly, government will be a large user of the electronic transmission of transfer payments, and the choices it makes from the alternative types of payments services will influence the standards chosen by the industry. In setting standards, however, we must be careful not to act precipitously

or allow market participants to use government regulation as a means of gaining inappropriate advantage over their competitors.

Second, when government must act, we must be careful to work with market forces. Rather than prescribing the means by which private firms pursue a public policy goal, government should articulate the goal and, as much as possible, permit the private sector to develop the means to pursue that goal. For example, bank regulators work to ensure that banks adopt systems and controls that measure, monitor, and control risk-taking. That goal is coincident with the objectives of the bank's owners, and the bank chooses the means of pursuing the goal.

Third, we must remember that we are public servants. Government should be extremely wary of imposing requirements solely for its administrative convenience. When applying auditability requirements to electronic payments systems that are designed to facilitate tax collection or the prosecution of certain laws, for example, we should weigh the cost against the resulting public benefit.

Fourth, we must maintain a modern regulatory infrastructure. To do that, we must determine which of our existing rules continue to be relevant in the world of electronic banking. We might reconsider, for example, how regulations that are based on geographic restrictions apply in such a world. If our rules are obsolete, we must modernize or eliminate them.

I believe these principles can guide us as we think about how to address concerns about the growth of electronic payments systems.

Concerns Raised by the Growth of Electronic Payments

Innovations in electronic payments technology raise a number of important concerns, which both the government and the private sector have articulated. Some of these concerns represent immediate problems that could prevent electronic payments systems from progressing further. Other concerns are less immediate, and become important only if electronic payments gain wider acceptance and become important payment vehicles. Still other concerns will become important in the longer term, and only if electronic payments systems come to dominate the current paper-based system.

Near-Term Concerns

Of immediate concern is the need to ensure that all participants have basic information about the rules governing the use of electronic payments. For example, participants need to understand who is liable if they lose a smart card or if a transaction is intercepted *en route*, or how electronic payments for which funds are unclaimed will be treated. Issuers and processors of electronic payments need this information to make basic business decisions, such as what type of accounting system to establish, or to determine the necessity of security devices for processing transactions. Such rules are likely to evolve without government intervention, like most other contracts for transactions between private parties. However, since the development of those rules

will influence the acceptability of a means of payment, and the public may have the expectation that it will be protected, government may find it in the public interest to make some of those rules clear.

A further significant concern is that electronic payments technology may create new ways to commit money crimes. If the dollar value and volume of money laundering, embezzlement, counterfeiting, or theft through breaches of electronic security increases significantly, the resulting loss in the efficiency of the payments system could create a drag on the economy.

Consumer Protection

In the area of consumer protection, there are at least three major areas of concern: security of the value in individual deposit accounts that are linked to smart cards or accessed electronically, protection of private information, and recourse in case of unauthorized use. Some observers warn that new electronic payments vehicles could make unauthorized use of credit lines and bank accounts much easier. For example, a lost or stolen smart card or home banking personal access code could lead to substantial losses for individuals or businesses.

To a certain extent, however, current payments mechanisms have raised, and successfully addressed, these issues. The use of credit cards to make remote purchases through telephones and wire services has gained wide acceptance among consumers and businesses, because protections exist to make those transactions secure. In the realm of electronic payments, industry has a strong incentive to create successful security devices and to build confidence in those payments mechanisms.

Electronic banking over computer networks may also create a new avenue for unauthorized access to private information. Certain controls that exist to address privacy concerns in the context of credit cards, credit agencies, and banks can be applied to electronic payments. In addition, to build necessary customer confidence, private sector providers are well aware that they must protect the financial information that travels on these networks. For example, Netscape Communications Corporation acted quickly to address the recent breach of its encryption system, and government intervention probably would not have provided a better solution. As the volume of transactions occurring on the Internet grows, however, government may need to address the increased need for security.

Also, as I have noted, government has the responsibility to ensure that its laws and regulations are kept up-to-date. Existing law should not be applied in a manner that would inappropriately discourage the development of electronic payments vehicles. For example, there are provisions of the Electronic Funds Transfer Act (EFTA), as implemented by Regulation E, that require banks to issue receipts for electronic transactions. As stated, however, it is unclear how those provisions apply to stored value card transactions or to the value stored on those cards. Hence, the OCC supports the legislation being considered by both the House and the Senate to clarify when the EFTA requires receipts for stored value card transactions. As proposed, the

provisions requiring receipts would not apply except in transactions where the card is actually used to access an account to effect a transaction from that account.

Safety and Soundness

As bank regulators, we must address the potential effect of increasing reliance on electronic payments on any or all of the risks embedded in all payments systems. Those risks include: credit risk, or the risk of default; systemic risk, which stems from the interdependence of parties using the system; transaction risk, the risk of loss from malfunctions in the operation of a transaction or settlement system; and fraud risk, the risk of loss from counterfeit claims, unauthorized use, or misappropriation of funds.

For example, the speed with which electronic payments can occur increases systemic risk by raising the possibility that a shock to the financial system would be transmitted rapidly to other parts of the system. A payments system that depends increasingly on a few, large communications networks or clearing houses could be more susceptible to the breakdown of that system, through either malfunction or sabotage.

Protections now exist for electronic funds transfers, which already account for most of the dollar volume of transactions in the U.S. economy. Such transactions tend to be large in value, but relatively small in number, however, so we must still consider whether a larger volume of small value transactions requires a new or different government response.

I am committed to ensuring that OCC supervision meets the challenges of any new technology, including electronic payments technology. To that end, we are devoting additional resources to the supervision of the new risks that developments in electronic payments technology may pose. OCC staff are working to increase their knowledge about all aspects of the new technology, and we are studying private sector efforts to introduce electronic payments technologies. A cadre of OCC examiners is continuing to specialize in the supervision of bank information systems and the risks associated with emerging technologies.

Finally, a number of private firms that are seeking to establish electronic delivery systems or to provide banking services over the Internet may soon apply formally to engage in the proposed activities and to create new banking institutions to engage in the activities. In considering those new activities, the OCC may have to modify its existing procedures for evaluating applications.

Access to Banking Services

The evolution of electronic payments technology introduces some new aspects to the continuing problem of access to banking services. Some observers believe that if electronic payments systems become widespread, the poor and the uneducated will be excluded from the payments system and hence, from our economy. They fear that a significant fraction of society will be unable to share in the cost savings, security, and increased convenience accruing from new

payments technologies because some forms of electronic payments require access to bank accounts, and many of the poor do not have banking relationships. Another concern related to access stems from the fact that all forms of electronic payments require that consumers have access to automatic teller machines (ATMs), personal computers, smart card machines, or enhanced telephones or televisions. Government should think carefully about the impact of emerging payments systems on the disadvantaged.

It is not obvious that the net effect of emerging electronic payments technologies on the poor would be negative. By reducing the cost of banking transactions sufficiently, the new technology could increase the availability of certain transaction services. In addition, some state and local governments have begun to distribute transfer payments electronically, and the Treasury is implementing a similar system for federal transfer payments. The electronic distribution of government benefits could be more secure and more convenient for recipients. When the recipient does not have a direct banking relationship, distribution of benefits on smart cards or through debit cards that access a government bank account might offer safety and convenience heretofore unavailable to the disadvantaged.

Furthermore, while the cost of some of these devices may put them beyond the reach of many individuals today, their cost has declined rapidly as technology has advanced. Advances in technology have already allowed banks to extend some services to wider areas through ATM networks. Telephone banking can extend that reach even further. It is highly likely that those costs will continue to decline as electronic payments technology advances, perhaps even reducing the total cost of transactions to below what they are today. Furthermore, even if electronic payments come to dominate existing forms of payment, it will be some time before that occurs. It is also likely that currency, checks, and credit cards will continue to be used as a means of payment.

Money Crimes

Most observers agree that new electronic payments technology brings new opportunities to commit money crimes, such as counterfeiting or theft through breaches of electronic security, in the U.S. and abroad. The new technology may lower the cost of committing these crimes by making it easier to disguise the proceeds of those crimes or to launder money.

In the past, to discourage money crimes, government has used reporting requirements, like those in the Bank Secrecy Act, and it has limited the availability of large denomination bills. In general, the ideas behind these measures probably can extend to electronic payments, but adapting them may be difficult and costly in some cases. Particularly with respect to security concerns, however, industry has the same incentives to solve these problems as the government. The public will not want to use these technologies unless the problems are addressed.

New electronic payments vehicles also raise auditability issues, which include the applicability of the reporting requirements in the Bank Secrecy Act and reporting requirements for international transfers of monetary instruments to electronic payments. Such issues must be

addressed, or federal, state and local governments could find it more difficult to collect tax revenues at home and abroad.

Longer-Term Concerns

In the longer term, if the number or dollar volume of electronic payment transactions grows to dominate the payments system, the financial system will face great challenges. Another concern relates to the anti-competitive effects of potential monopoly power within the payments system.

Another issue that further growth of electronic payments vehicles in our economy would raise is who should be permitted to issue electronic money. Traditionally, the federal government has retained control over money creation through its regulation of the banking industry. The potential extension of electronic money creation to nonbank firms raises many questions, including the applicability of the conventions and protections embedded in current banking laws and regulations to nonbank activity.

Government would also need to address the potential loss of seignorage if electronic payments are privately issued and replace currency.

Anti-Competitive Effects

The start-up costs associated with electronic payments technologies can be high. For example, smart card usage would require, at the very least, that banks and merchants install new card readers, and home banking would require large investments in computer software to make transactions secure. Those large fixed costs have led some observers to warn that a few financial services providers--those with the resources to absorb those costs--could come to dominate the payments system.

The consortia forming to develop, test, and market the various electronic payments vehicles provide some evidence to support this view. Some of these consortia combine traditional financial services providers with software providers, telecommunications companies, and electronic equipment manufacturers. Theoretically, the long-run effect could be a small number of firms selling limited services at higher prices. The threat of selective price cutting could discourage new entrants. It is also possible that the high fixed costs of establishing a network for electronic payments could encourage substantial consolidation of the banking industry.

I note, however, that the emergence of monopoly power in the provision of payment services will not occur unless there is a large-scale substitution of a new electronic means of payment for existing payments media. This is unlikely to happen soon. Instead, we are more likely to see an evolving industry structure that encompasses several payments vehicles, including some existing vehicles and a few new ones.

There is also some evidence to support another view: that the development of electronic banking might actually increase competition in banking markets and lower costs. Electronic banking offers an inexpensive alternative to branching to expand a bank's customer base, and many banks are using it to increase service to their customers. Many banks have started home pages on the Internet, and many plan to offer banking services over the Internet. Some banks are already offering certain banking services over the telephone. Smart cards and other forms of electronic cash could be the key to consumer acceptance of home banking, eventually allowing banks to reduce their physical branches.

Monetary Control

Government must also address the potential effects of electronic payments on macroeconomic stability, including their implications for the conduct of monetary policy. While these issues are primarily within the province of the Federal Reserve System, their resolution clearly affects the condition of banks and the banking system.

Broad concerns regarding the implications of electronic payments for monetary control include whether such developments in the payment system affect the Federal Reserve's ability to measure and influence both the amount of money in the economy and its speed of circulation. If so, the conversion to electronic payments could theoretically threaten the government's ability to conduct monetary policy by reducing the strength and reliability of existing monetary policy tools.

When new means of payment arise, existing measures of the money supply become outmoded, weakening the information content of those measures. As I am sure the Subcommittee is aware, the central bank has faced this problem many times. Over the past thirty years, we have seen a multitude of new payment vehicles--negotiable order of withdrawal (NOW) accounts, money market mutual funds, and credit card transactions--that have changed the ways individuals and businesses make payments. These changes have required the central bank to change how it measures money. The widespread adoption of electronic money potentially poses another such challenge for the central bank.

Some observers have noted that permitting nonbanks to issue electronic cash could weaken the Federal Reserve's influence over the money stock. Authorizing nonbanks to engage in fractional reserve banking without being subject to the same reserve requirements as banks could seriously complicate monetary control, if such balances became large relative to traditional measures of the money stock.

Conclusion

The technology to support the continuing progression in electronic payments vehicles is likely to continue to evolve, offering many gains for all segments of our economy. Ultimately, the market will decide whether these innovations succeed, and whether electronic payment vehicles will come to dominate the payments system. Government's role is to protect the public interest, ensure the efficiency and competitiveness of our markets, and maintain public confidence

in our financial institutions and payments system. As Comptroller and coordinator of the Treasury Department's efforts on electronic payments issues, I am committed to ensuring that we carry out that role efficiently and in conjunction with market forces. I am also mindful that the electronic payments area is evolving rapidly, and I am committed to vigorously following the developments in this area to ensure that the public interest is protected.

Whatever the outcome, there will be a significant transition period before electronic money gains broad acceptance. The private sector and government must use this transition period to address the concerns that will inevitably arise as innovation continues.

For release on delivery
10:00 am, EDT
October 11, 1995

Statement by

Alan S. Blinder

Vice Chairman

Board of Governors of the Federal Reserve System

before the

Subcommittee on Domestic and International
Monetary Policy

of the

Committee on Banking and Financial Services

U.S. House of Representatives

October 11, 1995

I appreciate this opportunity to present the views of the Federal Reserve Board on issues raised by various emerging electronic payment technologies that go under such names as "digital cash" or "electronic money." Spurred by recent advances in computing, communications, and cryptography, this nascent industry holds the promise of improving the efficiency of the payment system, particularly for consumers.

While the potential for exciting developments in this field is certainly there, we should all keep the latest round of innovations in historical perspective. First, the concept of "electronic money" is not new; electronic transfer of bank balances has been with us for years. Indeed, some of the new proposals simply make available to consumers and smaller businesses capabilities that large corporations and banks have had for many years. Second, no one knows how this industry will evolve--either qualitatively or quantitatively. Some of us, for example, can recall predictions made a generation ago that the United States would soon be a cashless, checkless society.

This last point reminds us that, at present, we do not know which, if any, of the many potential electronic innovations will succeed commercially. In this testimony, I will concentrate on stored-value cards and other types of so-called "electronic cash" because they seem to raise the most challenging public policy issues. In particular, depending on their design, they could amount to a new financial instrument--an electronic version of privately issued currency. But even the concept of private

currency is not entirely new. Travelers checks are, of course, familiar to everyone. And in the nineteenth century the United States had considerable experience--not always happy--with private bank notes. But widespread use of private electronic currency would certainly raise a number of policy questions.

On behalf of the entire Board, I want to state clearly at the outset that the Federal Reserve has not the slightest desire to inhibit the evolution of this emerging industry by regulation, nor to constrain its growth. On the contrary, the Board has and will continue to encourage innovations in payments technologies that benefit consumers and businesses. I am here today to raise questions, and to bring some issues to the attention of Congress, not to provide answers. Given the considerable uncertainties surrounding the design and ultimate usage of these products, it is far too soon for answers.

Nonetheless, it is not too early to begin thinking about a number of interesting and complex issues which may be raised by electronic currency. These include the impact on federal revenues, the legal and financial structure for these products, risks to participants, the application of consumer protection and anti-money laundering laws, and some issues related to monetary policy. Some of these issues may need to be addressed by the Federal Reserve and other regulatory agencies and some by the Congress. Some may need prompt attention, while others can wait. The present is, we believe, an appropriate time

for public debate and discussion, a poor time for regulation and legislation.

Seigniorage and the Budget

Let me start with a potential revenue issue that will arise if the stored-value industry grows large. The federal government currently earns substantial revenue from what is sometimes referred to as "seigniorage" on its currency issue. In effect, holders of the roughly \$400 billion of U.S. currency are lending interest-free to the government. In 1994, for example, the Federal Reserve turned over about \$20 billion of its earnings to the Treasury, most of which was derived from seigniorage on Federal Reserve notes.

Should some U.S. currency get replaced by stored-value products--which are private monies--this source of government revenue would decline. Indeed, one of the major economic motives for institutions to issue prepaid payment instruments is to capture part of this seigniorage, just as issuers of travelers checks do now. Because the demand for stored value products and the degree to which they will substitute for U.S. currency is totally unknown at present, the loss of seigniorage revenue is impossible to estimate. It is likely to be small. But it is something Congress should keep an eye on.

We should not, by the way, jump to the conclusion that the government's lost seigniorage will go to the companies that issue stored value--though that will probably happen at first. It may be technically feasible to pay interest on stored-value

products. To the extent that competition forces issuers of these products to pay interest, the lost seignorage will accrue to holders rather than issuers.

This discussion raises the question of whether the federal government should issue electronic currency in some form. (In posing this question, I refer to general-purpose stored-value cards, not to special-purpose instruments such as government benefit cards which, in our view, do not raise major issues.) Government-issued electronic currency would probably stem seignorage losses and provide a riskless electronic payment product to consumers. In addition, should the industry turn out to be a "natural monopoly" dominated by a single provider, either regulation or government provision of electronic money might be an appropriate response.

But such a conclusion seems quite premature. And the availability of alternative payment mechanisms would mitigate any potential exercise of market power. Further, government issuance might preempt private-sector developments and stifle important innovations. Finally, the government's entry into this new and risky business might prove unsuccessful, costing the taxpayer money. So, while we would not rule out an official electronic currency product in the future, the Federal Reserve would urge caution.

Legal and Regulatory Structures

One area that may need prompt attention from both policymakers and the industry is clarifying the legal and

regulatory structure that will govern electronic money products. In this case, failure of the government to act may, ironically, impede rather than facilitate private-sector developments.

As with other payment mechanisms, issuers and holders of electronic currency take on some degree of ongoing credit, liquidity, and operational risks. The risk to a consumer using a stored-value card for small "convenience" purchases may be inconsequential. But such risks can become significant when larger amounts of money become involved--for example, when merchants and banks accumulate and exchange significant amounts of stored-value obligations during the business day.

Risks to participants arise from a number of sources. Cards might malfunction or be counterfeited. Issuers might invest the funds they receive in exchange for card balances in risky assets in order to increase their earnings. But riskier investments can turn sour, possibly impairing the issuer's ability to redeem stored-value balances at par and imposing losses on consumers and other holders (if the obligations are not insured). Further, the clearing and settlement mechanisms for stored-value cards and similar products--if they become widely used--could generate significant credit and other settlement risks.

We believe that both the industry and the government should focus on answering several mundane questions that seem to be receiving little attention amid the continuing publicity about these products. For example:

- Whose monetary liability is the particular form of electronic money?
- If an issuer were to become bankrupt or insolvent, what would be the status of the claim represented by a balance on a card or other device?
- In such a situation, when and how would funds be made available to the holder?
- Who is responsible for the clearing and settlement mechanism?

Developers of these products have discussed a variety of possible options, but the industry does not appear to be converging on one or more models that would be transparent and readily understood by users. In addition, there is no specialized legal framework for stored-value transactions, as there is for checks and other common retail payment mechanisms. For example, state or federal law specifies when an obligation is discharged by cash, check, or wire transfer--but not if payment is by stored value.

From the Federal Reserve's perspective, new and exciting technological developments in payments mechanisms should not overshadow the conventional and ongoing need for clear and soundly based legal and financial arrangements. It is essential that developers and issuers clarify the rights, obligations, and risks borne by consumers, merchants, and other participants in new systems before these products are widely introduced.

The need to attract and retain customers will naturally drive developers and issuers of electronic money products toward investment policies and operational controls that make their products useful and safe. So, to some extent, the market will be self-policing. Nevertheless, it could be costly and difficult for consumers and merchants to monitor and evaluate the safety of electronic money products, especially given their technological complexity. So the government is likely to become involved as well.

To guard against financial instability and to protect individual consumers, the government has, in the past, mandated a range of regulatory measures for private financial instruments. Three principal approaches are used:

1. Disclosure and surveillance: In the case of mutual funds, securities laws generally require disclosures about asset holdings. Audits and examinations of investment funds also help ensure that reported assets are actually held.

2. Portfolio restrictions: In some cases, standards or restrictions on portfolios help limit the riskiness of the assets. Money market mutual funds, travelers checks in some states, and, historically, privately issued bank notes are familiar examples.

3. Government insurance: Balances in depository institutions, of course, receive the most comprehensive protection mechanism available: federal deposit insurance.

At some point, though certainly not now, Congress will have to decide which, if any, of these protection mechanisms should be applied to stored-value products.

For example, if stored-value obligations of banks are treated as insured deposits--which is, by the way, another legal question that needs to be cleared up--then credit risk is effectively transferred from consumers to the government. In fact, the European central banks have gone so far as to recommend that only banking institutions be permitted to issue prepaid cards, presumably because that gives such cards the same degree of protection and financial oversight as traditional bank deposits.

The Federal Reserve Board has not viewed such a restrictive policy as appropriate. But the regulatory structure for electronic money products does merit further analysis. At a minimum, we believe that issuers of stored-value cards and similar products should clearly disclose the various risks that holders bear, including their coverage, if any, by deposit insurance.

Consumer Protection and Law Enforcement

The question of whether and how to apply the Electronic Fund Transfer Act (EFTA) and the Federal Reserve's Regulation E to these products has received considerable attention from industry participants, at the Federal Reserve, and in Congress. Among other things, Regulation E limits consumers' liability for unauthorized electronic withdrawals from their accounts, provides

procedures for resolving errors, and requires institutions to provide disclosures, terminal receipts, and account statements. Uncertainty regarding the application of Regulation E may be holding back the development of the industry, and resolving this question would help clarify some of the major risks that consumers may bear.

H.R. 1858 would exempt all stored-value cards and a potentially wide range of other products, including transactions through the Internet, from the EFTA and Regulation E. The industry seems worried that, without such an exemption, the Federal Reserve will apply Regulation E in a heavy-handed manner. On behalf of the Board, I would like to assure industry participants and this Committee that we have no such intention. The Board recognizes that some of the requirements of Regulation E should not be applied to certain of these new payment products. For example, it makes little sense to require either printed receipts at ordinary vending machines or periodic statements detailing small transactions.

It seems premature, however, to legislate a blanket exemption from EFTA without first exploring some of the basic issues raised by these new payments mechanisms. Disclosure policy is a good example. If a consumer who loses a stored-value card with a balance of several hundred dollars is not entitled to a refund, he or she should know this when the card is purchased. In this case at least, Regulation E requirements could be beneficial at minimal additional expense. The Federal Reserve

would like to develop, and then put out for public comment, proposals for applying parts of EFTA, such as appropriate disclosures, to stored-value cards--and for exempting them from the remainder. We would hope to be able to accomplish this within a few months.

Another issue related to consumer protection is privacy. While physical cash leaves no audit trail, many electronic currency products would. Such a trail may be desirable for certain purposes. But consumers would almost certainly be concerned if each purchase from a vending machine was recorded for possible reporting to marketers and others. Privacy is not a traditional Federal Reserve issue, but we do think it should be of concern to members of Congress.

The mention of privacy leads naturally to some potential, future law-enforcement concerns. While we would caution against establishing restrictive rules that could stifle innovation, the eventual opportunities for money laundering using electronic products may be serious. At present, the menu of new products proposed for distribution in the United States holds little appeal for illicit activities due to their relatively low balance limits, the potential audit trail, and their limited acceptability as a means of payment--at least in the near term. In fact, most of the proposed stored-value products are not designed to circulate freely like currency, and thus should be of limited concern to law-enforcement authorities. Over the longer term, however, it seems possible that electronic mechanisms that

can hold large balances and make large untraceable transfers over communications networks could become attractive vehicles for money laundering and other illicit activities--especially if they are widely used and bypass the banking system. Existing anti-money-laundering regulations may then need modification.

A related side issue is the possibility that nonbank entities could offer banking services illegally over the Internet. Using the term "bank" to market banking services without an appropriate license is generally a violation of federal or state laws. But new electronic technologies may challenge both traditional definitions of "banking services" and the ability to enforce existing laws. At some point, therefore, Congress and state legislatures may want to review the basic legal concepts that define banking and their methods for preventing fraud and unlicensed banking activity. Because electronic messages show little respect for national borders, these issues will likely require the coordinated attention of the banking authorities in various countries.

Monetary Policy Issues

Finally, let me say a few words about monetary policy. Concerns have been expressed that introducing what amounts to a form of private currency might damage the Federal Reserve's control of the money supply and lead to inflationary pressures. I can assure you that this is most unlikely. The Federal Reserve currently issues or withdraws currency passively to meet demand, adjusting open-market operations accordingly to keep monetary and

credit conditions on track. We would presumably continue to do this if private parties began issuing electronic currency which reduced the demand for paper currency.

In any event, electronic currency, if it grows large, will be only one of several changes in financial markets in the years ahead. Some of these may change the details of how monetary policy is implemented, just as financial innovations have in the past. We believe we have the capability of adjusting to these changing circumstances while continuing to meet our traditional responsibilities for economic stability.

However, there is a technical issue relating to our reserve requirements. Depository institutions are required to maintain reserves, either in cash or on deposit with Federal Reserve Banks, in proportion to their outstanding transaction accounts. Under current regulations, stored-value balances issued by depository institutions would be treated as transaction accounts and hence subjected to reserve requirements; the Board will need to review this treatment as stored-value devices come into use. But the Federal Reserve does not currently have the authority to impose reserve requirements on non-depository institutions. Thus there is a potential issue of disparate treatment of bank and nonbank issuers.

Depository institutions benefit from their access to the federal safety net; but they pay for this privilege by being subject to reporting obligations, reserve requirements, regulation, and supervision by the banking agencies. Nonbank

issuers are free of most such burdens, and hence may have a competitive advantage over banks in certain product lines. The Federal Reserve has often expressed concern in the past about potential competitive inequities that disadvantage banks. But because of the pervasive uncertainties that I emphasized at the outset, it is far too early to have any useful insights into the implications of this disparity. We simply want to call it to your attention.

Conclusion

In summary, it is clear that new electronic payment products raise a number of diverse policy issues, both for Congress and for the Federal Reserve. I have not had time to mention them all here. But, at this point, the uncertainties regarding the future of "electronic money" are so overwhelming that we mainly suggest patience and study rather than regulatory restrictions. We do believe, however, that certain rules need to be clarified and future developments should be monitored closely. We look forward to working with Congress and other regulatory agencies in this regard.

STATEMENT
of
STANLEY E. MORRIS
DIRECTOR
FINANCIAL CRIMES ENFORCEMENT NETWORK
UNITED STATES DEPARTMENT OF THE TREASURY
before the
SUBCOMMITTEE ON
DOMESTIC AND INTERNATIONAL MONETARY POLICY
of the
COMMITTEE ON BANKING AND FINANCIAL SERVICES
U.S. HOUSE OF REPRESENTATIVES
October 11, 1995

Mr. Chairman and members of the Subcommittee, I am Stanley E. Morris, Director of the Financial Crimes Enforcement Network called "FinCEN." Your series of hearings concerning the future of money are timely and very important. I am very pleased to have been asked to participate.

Two weeks ago, FinCEN sponsored a Colloquium on cyberpayment systems at New York University Law School. We brought together more than 125 people--financial services providers, software developers, academics, consumer representatives, and regulatory, policy, and law enforcement officials--to speak face-to-face about the evolution of advanced electronic payment systems. Our attendees included a number of people who appeared before this Subcommittee on July 25, as well as the Comptroller of the Currency, Under Secretary Noble, senior officials of the Federal Reserve Board and of the Treasury, and a member of your subcommittee staff.

The message we received at the Colloquium is the one you heard in July and have heard today--that advances in the design and implementation of the new payment systems are among the most complex and potentially far-reaching developments generated by the "age of the intelligent machine."

Today, I want to address possible elements of the new systems that cause concern for officials responsible for fighting money laundering and financial crime.

Note that I refer only to "possible" elements of the new systems. The systems don't have a common architecture or terminology. And representatives of the industry with whom we have spoken are alert to the risk that their systems could be misused. They are willing to work with government to do something about the risk.

I also want to emphasize that the fact that we are thinking about the new technology does not mean that we are against it--just the opposite. It means that we are keenly aware of our need, indeed of our responsibility, to understand the technology first, before deciding if there are law enforcement issues that require resolution.

A sense of FinCEN's mission--and of its evolving partnership with the financial community--helps to frame our perspective on the new systems. FinCEN establishes, oversees, and implements Treasury policies to prevent and detect money laundering. It administers the Bank Secrecy Act, or "BSA," which is the core of those efforts.

Our interest in the new systems reflects our own responsibilities as a regulator. The BSA requires recordkeeping and reporting by more than 200,000 financial institutions of all kinds and creates the largest currency transaction reporting system in the world. We have already been asked whether and how the BSA applies to the new systems, and as a result, we have come to recognize--as have you and many others--that the systems' potential uses raise issues that go beyond the jurisdiction or mission of any particular agency.

That range of issues is another reason FinCEN is involved. As its name indicates, FinCEN is itself a "network;" it serves as the nation's central point for broad-based financial intelligence and information sharing for federal, state, and local law enforcement and financial regulatory agencies. To make its own network more effective, FinCEN strives to bring enforcement agencies and the private sector together wherever it can, to create cost-effective measures to prevent and detect financial crime.

As FinCEN's Director, I am keenly aware of the potential impact that the new technologies can have on the work of financial investigators. Let me explain.

Financial investigations are recognized as the key to combating narcotics trafficking and organized and white collar crime. But such investigations are extremely difficult to carry out. First, it takes many years of working in the financial industry to understand all its intricacies. Second, no single agency possesses a sufficiently broad or cross-jurisdictional focus and information base to track financial movements; and third, the sheer size, variety, and pace of change of the financial sector make financial investigations ever more difficult.

Our strategies to deal with these difficulties have historically centered on eliminating "bank secrecy." Treasury has administered the BSA, as Congress intended, to require record keeping that would preserve a financial trail for investigators and to require reporting of significant

currency transactions, and transportation of currency and monetary instruments into and out of the United States.

For the past two years, building on legislation which originated in this Committee, we have worked diligently to "re-engineer" the BSA, enlisting proactive support of industry, cutting out unneeded regulation, and simplifying what remained. A cornerstone of our approach is the reporting of truly suspicious transactions, cutting way back on mechanical reporting that is often far more costly than its usefulness justifies.

The investigator's motto-- "follow the money," relies on the need of criminals to move funds through the financial system to hide and use the proceeds of their crimes. Currency is anonymous, but it is difficult to handle and to transport in large amounts. Anyone who has seen a pallet of newly printed bills on a tour of the Bureau of Engraving and Printing, or, better still, has seen a photograph of a drug cartel's counting house or currency stashes, knows what I mean.

A large amount of currency, like an elephant, is difficult to hide. It takes time to move and attracts attention. Attention is the enemy of criminal activity.

The new payment systems have the potential to change all this. If cards can be "loaded" with value not just from banks, but from retail outlets or other sources, current systems for tracking funds could lose their value. Internet-based systems for transferring large amounts or a

way to store large sums on a "smart card" that would be recognized as "carrying" dollars at any place in the world pose the same risks.

Our reasons for concern do not stop with asking whether such transfers are transfers of "currency." The question is not to make sure we get a report simply to get a report. The new systems combine the speed of the present bank-based wire transfer system with the anonymity of currency--they create the best of both worlds. They make wire transfer equivalents anonymous, and they make currency easy to move around the world at almost the speed of light. Smart card transactions and international payments transacted over the vast Internet system could be immediate, potentially anonymous, effected in multiple currencies, and conducted entirely outside of the traditional funds transfer channels.

Is that necessarily bad? Not at all. In fact, far from it. At the Colloquium, Under Secretary Noble used an example I'd like to repeat: a U.S. retailer, let's say a shoe store, could accept smart cards for purchases. As the store's revenues increase, it could transfer the value of its revenues to a smart card or download the value into a computer. This value could in turn be transferred through the Internet to financial institutions or people around the world to pay invoices, order materials, or pay suppliers--in all cases stimulating commerce, making trade less expensive, and providing benefits to consumers.

The same systems can benefit consumers in other ways. They can reduce the hazards and inconvenience of carrying cash, and they can provide a significant degree of protection, via smart card technology, for those who do not have bank accounts. They can foster electronic commerce, and they can reduce the costs of processing cash by retailers and the risks of robbery for merchants in all areas.

But, as I have pointed out, the same efficiencies could, at least in theory, create opportunities for serious exploitation by money launderers. Suppose my Internet user is a narcotics trafficker or an agent for a gang of sophisticated criminals of any other sort. Consider the invoices the trafficker might pay, the supplies he might order and the transactions he might accomplish if, for instance, he could download an unlimited amount of cash from a smart card to a computer, and then transmit those funds to other smart cards in locations around the world--all anonymously, all without an audit trail, and all without the need to resort to a traditional financial institution.

History has shown us that as we invent new technologies, criminals are waiting on the periphery to use them--trains produce train robbery, telephones create telephone frauds, air craft hijacking and terrorism. In the same way, the possibility of virtually untraceable financial dealings, if it came to pass, would create new, but this time, perhaps unparalleled problems for law enforcement. Those of us who have fought so hard to end bank secrecy as a convenient

excuse around which criminals can cluster will have won little if we now turn to a world in which financial institutions can easily be bypassed via the Internet or use of the telephone lines.

That leads to an important point about money laundering and related financial crimes. They all involve taking acts that are themselves, in isolation, not only legal but commonplace-- opening bank accounts, wiring funds, and exchanging currencies in international trade. Given that basic fact, we have few ways now to separate the malefactors from the businessmen. The new technologies will give us even fewer ways, unless we work with their developers.

How should we do so? I'll tell you frankly, I don't know yet. Technology raises the stakes in many ways and for each risk there is a benefit.

For example, I would be concerned if the new systems permitted encryption of large financial transactions in a way that would make their detection or the identification of the sending or receiving parties incapable of reconstruction, in certain cases. But encryption is vital to protect the security of electronic commerce and financial transfers, and sophisticated encryption is already in place, of course, in the interbank transfer systems. And I recognize the uses of encryption to protect privacy that consumers feel is threatened by the computer age.

We are not without tools to deal with issues as they develop, although I frankly don't know yet whether those tools will be adequate. As I indicated earlier, the BSA authorizes the

Secretary of the Treasury to require recordkeeping by financial institutions and to require reports of suspicious transactions and currency transactions. The BSA also requires the registration of money transmitters. How do these concepts apply to the new systems?

Reporting of cross-border transportation of currency and monetary instruments in excess of \$10,000 is also required by the BSA. How should that requirement be applied to smart cards shipped or carried across the border? To Internet transactions using the new systems?

Here are some of the questions we will be asking:

-- Do the systems create and maintain an audit trail?

-- Does that audit trail extend beyond the initial transaction to subsequent transactions in the chain?

--What are the privacy implications of that audit trail?

--Will the systems be restricted to transactions below a certain dollar amount--a cap, if you will?

--Will the systems permit effective and timely monitoring of suspicious transactions, for example, repeated multiple transactions designed to evade dollar caps?

-- Are the cyberpayment systems being offered by or through a regulated entity?

--Do the systems permit self-contained, person-to-person transactions without the involvement of a financial institution or other regulated entity?

We don't know enough yet to make good decisions. We may need this Committee's assistance in dealing with the questions I've raised, but the time is not yet right to ponder whether additional legislation is required.

Too often, government regulators have attempted to thwart a potential criminal threat by imposing burdensome regulations that reflect little appreciation of the nature of the threat, or the business practices of the affected industries. We cannot make the same mistakes with cyberpayment systems. The technology is developing too rapidly, and the gains and efficiencies potentially created by the new systems are too important. At the same time, without thoughtful and balanced approval of law enforcement concerns now--before criminals begin to exploit the new technology--the prospects for abuse by organized crime, money launderers, and other financial criminals could be too great.

What does the "cyber-future" hold for FinCEN? Candidly, we are still sorting through the wealth of information, recommendations, and comments received at our Colloquium. We're working hard to support the Comptroller as he coordinates Treasury's efforts. I'm very pleased that the Defense Department's Advanced Research Projects Agency has awarded a contract to KPMG Peat Marwick to assist FinCEN in continuing its work.

That leads to a final point. This new technology requires a proactive approach from law enforcement, and I think FinCEN is in a position to assist in working out the issues raised in today's hearing. We were created in the recognition that financial crime is a problem and that it can only be alleviated by bringing together resources from many areas and leveraging their impact. In the same way, I hope that we can serve as a "network" that enables law enforcement and financial compliance officials, technology developers and bankers, to work out the details of solutions to some of the potential problems I've outlined.

We do not want to impede the development of technologies that can benefit us all. Our goal is simply to try to inoculate the new systems against crime and misuse by criminals - to permit their healthy growth into the next century.

So our task is just beginning. We look forward to working with you, and in that spirit I welcome your questions.



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON D.C. 20503

ADMINISTRATOR
OFFICE OF
INFORMATION AND
REGULATORY AFFAIRS

STATEMENT OF SALLY KATZEN
ADMINISTRATOR
OFFICE OF INFORMATION AND REGULATORY AFFAIRS
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
SUBCOMMITTEE ON DOMESTIC AND
INTERNATIONAL MONETARY POLICY
U.S. HOUSE OF REPRESENTATIVES

October 11, 1995

I am pleased to appear before the Subcommittee on Domestic and International Monetary Policy today to participate in your hearing on the security of electronically transmitted financial information.

As you know, the Clinton Administration is a strong proponent of the rapidly evolving National Information Infrastructure (NII), the high-speed telecommunications networks, databases, and advanced computer systems that will make electronic information widely available and accessible. For the most part the NII is being designed, built, owned, operated, and used by the private sector. The government has a significant role to play, but clearly not the primary one. The NII includes the Internet, the public switched network, and cable, wireless, satellite communications, and public and private networks. As these elements become increasingly interconnected and interdependent, individuals, organizations, and governments will use the NII to engage in multimedia communications, buy and sell goods electronically, share information holdings, and receive government services and benefits.

We all recognize that in addition to presenting new opportunities, the NII is also presenting new challenges. To capitalize on those opportunities and to face the challenges, the Administration in 1993 formed the Information Infrastructure Task Force (IITF), chaired by Secretary of Commerce Ronald H. Brown, to coordinate Federal activities related to the NII. The IITF consists of three primary committees: Telecommunications Policy, Applications and Technology, and Information Policy, and a number of working groups and subcommittees. I chair the Information Policy Committee, as well as a more specialized interagency group -- the NII Security Issues Forum -- that coordinates security efforts across all elements of the IITF. It is in that latter role that I have become involved in the subject of today's hearing.

What I would like to do today is discuss our view of the problem of security on the NII, and some aspects of the Federal role in promoting that security. I will focus primarily on policy efforts being conducted under the umbrella of the IITF; using examples from ongoing Administration initiatives that relate to electronic financial information.

I. What is Security of the NII?

To begin with, let me describe what I mean when I use the term "security of the NII." Security is often thought of as synonymous with confidentiality -- that is, assuring that information will be kept secret, with access limited to appropriate persons. But in context of the NII, security has a meaning that reaches beyond confidentiality to include other attributes as well: integrity -- assuring that information will not be accidentally or maliciously altered or destroyed; reliability -- assuring that systems will perform consistently and at an acceptable level of quality; and availability -- assuring that information and communications services will be ready for use when expected.

These attributes focus on the systems -- the hardware/software, interconnections. What we have tried to do is to think of them from the perspective of an individual using the NII. The results of this exercise was five "security tenets," which characterize in layman's terms the security needs of users of the NII. We published them in the Federal Register in June having proposed them for public comment in early 1995 [see Vol. 60 No. 28 of the Federal Register, p. 8100]. The five tenets are:

- 1) the ability to control who sees (or cannot see) their information and under what terms;
- 2) the ability to know who they are communicating with;
- 3) the ability to know that information stored or transmitted is unaltered;
- 4) the ability to know when information and communication services will (or will not be) available; and
- 5) the ability to block unwanted information or intrusions.

Of course, the details of implementation of the tenets will vary by user -- whether teachers, doctors, or tax preparers -- and by application -- whether communicating over a two-way multi-media conference, sharing data between doctors and patients, or calculating a tax return. Furthermore, two caveats attach to these security tenets:

- 1) None is absolute. For each tenet there may be valid societal reasons -- such as an emergency or a need to protect another's rights -- that cause the tenet to be conditioned in some manner.
- 2) Each requires NII participants to take responsibility for establishing the terms and conditions under which they will exchange information. The distributed and empowering nature of this technology demands a greater level of personal responsibility from participants than when communications systems were more centralized and less powerful. Education of NII participants is thus a critical task.

We believe that security -- so defined -- is not a peripheral or inconsequential issue, but rather is an essential element of the NII. Without the confidence that information will go where and when it is supposed to go, and nowhere else, the NII will not be used to its fullest extent to support health, education, commerce, public services, and advanced communications.

II. Public Dialogue is Essential

This Administration is committed to maintaining an open dialogue with the public in developing the proper Federal role in maintaining, and improving security of the NII. This Subcommittee's hearings contribute to that dialogue. In 1993, the President established the U.S. Advisory Council on the NII, which includes representatives from industry, labor, State and local governments, and public interest groups, to advise the Secretary of Commerce on issues relating to the NII. One of three working groups of the Advisory Council is specifically addressing security issues of the NII.

Over the past year and a half, the Administration, in cooperation with the Council and other members of the public, has conducted seven public meetings attended by government officials and members of the private and public interest sectors. A general meeting was held in the summer of 1994, at which individuals representing business, manufacturing, banking, health, entertainment, publishing, education, libraries, and government services discussed their views of security needs in the NII. Subsequent sessions addressed the needs of various sectors using the NII. The subjects of those meetings were:

"Commercial Security on the NII," which focused on the need for intellectual property rights protection in the entertainment, software, and computer industries;

"Security of Insurance and Financial Information";

"Security of Health and Education Information";

"Security of the Electronic Delivery of Government Services and Information";

"Security for Intelligent Transportation Systems and Trade Information"; and

"The NII: Will It Be There When You Need It?", which addressed the availability and reliability of the Internet, the public switched network, and cable, wireless, and satellite communications services.

In addition to the NII-related meetings, the Administration is working closely with affected members of the public to support ongoing initiatives. For example, the Electronic Benefits Task Force has met with representatives from State governments, retailers and grocers, and client advocacy groups across the country. Many of the attendees at these meetings spoke strongly of the positive effect that EBT had on their self-esteem and in providing them greater

personal safety. EBT pilot projects in states such as Maryland, Texas, and Ohio have demonstrated EBT's ability to improve service delivery, prevent fraud, and reduce costs.

Provider and User Security Concerns

The public meetings solicited discussion from a broad range of NII participants, both providers and users of NII services. Regardless of the commercial, industrial, or public interest use represented, many of those attending shared concerns about: the potential inability to control secondary uses of information; a mistrust of government's use of information; questions of liability for loss or inappropriate access to or use of information; the desire to protect one's own system from outsiders, whether by hostile attacks or junk mail; and risk of system failure at times of critical need. The most frequently expressed concern was that personal information, such as information pertaining to an individual's finances, health, or purchasing habits, could be disclosed to, or manipulated by, an unauthorized user. These shared concerns are reflected in the security tenets I described earlier.

Some commenters called for the government to take an activist role, such as censorship of defamatory or pornographic information transmitted over the NII, or providing additional funding for national security and emergency preparedness programs. Other commenters seemed to prefer a lesser government role. For example, some desired open access to and use of virtually all information and systems without interference by the government. Others criticized the Federal government's export control policy, which requires export licenses for powerful cryptographic systems. Some commenters were suspicious of the technology underlying the NII and how it would be used. Some witnesses were also concerned that government's involvement could create greater inefficiencies, increase susceptibility to invasions of privacy and risk of fraud, and contribute to the depersonalization of society.

Moving from the general to the focus of this hearing, I would like to summarize the concerns and needs we heard regarding governmental systems and financial services.

Government Information and Services

Use of the NII is becoming integral to virtually every Federal program, and Federal agencies are increasingly relying on that use for execution of their missions. The NII supports programs as varied as air traffic control, compilation of the decennial census, response to natural disasters, and delivery of social security benefits. This use of the NII in Federal operations promises improved efficiency of governmental program delivery. However, it also introduces new security vulnerabilities. Addressing security vulnerabilities in our own operations is a direct responsibility of the Federal government, since such vulnerabilities could degrade Federal program effectiveness and control of Federal funds, and affect the integrity, confidentiality, and/or availability of government information.

At the public meeting on government services, the use of "smart cards" and magnetic strip debit cards for delivering food stamps was discussed in depth. Smart cards provide the advantage of on-time payment, increased dignity, and improved efficiency in program administration. However, cards can be lost or stolen. Other concerns include the potential for counterfeiting such cards or otherwise manipulating the value of the cards and concern that unauthorized access to individual purchasing records could violate personal privacy. Users of these cards need confidence that the benefits will be available when they expect them to be, and that associated information will not be abused by those with access to it.

Although government is one of the largest users of the commercial information infrastructure, it relies, and will continue to rely, almost exclusively on commercial private and public networks for many of its current and anticipated electronic transactions. For example, the Federal Electronic Benefits Task Force has concluded that the government should not build a new infrastructure to support EBT and should instead rely on the existing debit network infrastructure. Similarly, with the support of the President's Council on Integrity and Efficiency, the government expects to rely on the commercial infrastructure for meeting the security needs of EBT.

Financial, Insurance, and Commercial Services

As noted above, one of our public meetings focused on another area of particular interest today -- financial, insurance and commercial services on the NII. As you know, the financial and insurance sectors have relied for decades on closed networks in order to transfer funds and share information. We heard concerns that as their networks become more open, new security tools and techniques will be needed to protect the confidentiality and integrity of valuable commercial information. Questions of liability will also arise if improper disclosure of customer information occurs while it is being transmitted over the public switched network. The advent of so-called digital cash involves different challenges. It requires a technical method to avoid forgery and authenticate the current owner. Yet, some witnesses favor the capability to execute anonymous transactions.

As consumers use the NII to conduct business, they will want to verify that a payment or order was received correctly. Without a face-to-face transaction to verify the authenticity of the customer and of the vendor, the potential for fraud increases for both parties, requiring methods of electronic notarization, digital signatures, and date-stamping. One witness pointed out that the vast majority of technical solutions address the issue of protecting an organization's data from individuals, while little attention has been paid to the problem of how the individual's data can be protected from organizations. This situation is illustrated by the way in which information about an individual's purchasing habits is bought and sold in private markets. Other personal information that is generally publicly available, such as marital status, home ownership, and status in legal proceedings, is collected by the private sector and sold as a commodity. Some individuals expressed a desire to exercise greater control over the use of this information or to be

reimbursed for its use. The IITF has developed principles to guide policy development in this area. These principles have been endorsed by the U.S. Advisory Council on the NII.

III. Findings and Recommendations from the Public Meetings

Based on comments we received at the public meetings, the Forum prepared a draft report, "NII Security: The Federal Role" and issued it for public comment in June of this year. I have attached a copy of the report to this statement. The draft report includes a set of proposed government actions to improve the security of the NII.

The public comment period ended last month. We are still in the process of analyzing the comments, but our initial impression is that the draft report was generally well received. There was no dispute that the government has an important role in NII security, particularly in areas such as assuring that criminal laws are effective and protecting its own systems that use the NII. In other areas, however, a number of commenters stated that the government should not be too intrusive. These commenters believe that the marketplace will provide needed security. This view is likely to be shared by the U.S. Advisory Council mentioned earlier.

I want to discuss three areas that have emerged in this public dialogue where it is clear that there is a governmental role and which bear on today's subject: 1) national and economic security concerns, 2) Federal use of the NII, and 3) use of cryptography.

1. National and Economic Security

As the United States as a whole becomes increasingly reliant on the NII for communications and information, key components of our infrastructure will become increasingly dependent on it. For example, the power grid, transportation systems, and financial institutions will all be tied into and hence dependent on the NII. Security weaknesses in the NII can place those infrastructure elements at risk. Accordingly, a significant attack on the NII would be a threat to our national and economic security in addition to the significant personal and economic harm it would cause. All Federal entities that oversee various parts of the U.S. infrastructure must be aware of the changing risk that increasing reliance on the NII entails. They also must be aware of the various types of threats to the NII and the magnitude of those threats, and they must do what they can to ensure the secure use of the NII by their overseen sector.

Thus, for example, the Transportation Department may need to adjust its regulatory oversight of aircraft to account for the risks involved in aircraft's use of the NII. Similarly, the Securities and Exchange Commission is adapting its oversight of securities exchanges, and the Treasury Department and the Federal Reserve Board have underway several initiatives to adapt their oversight of the nation's banking and financial system. I understand the Treasury Department and the Federal Reserve Board will be testifying today on their activities in assuring that their oversight of the banking system remains effective.

2. Federal Use of the NII

As noted earlier, the federal government is one of the largest users of the NII. The government uses the NII to interact with the public, and State, local or tribal governments to deliver benefits and services. The government also uses the NII for internal government purposes, such as for handling and communicating classified national security information.

The government relies heavily on the NII to disseminate information to the public. This Administration has made electronic information access and delivery a priority, and our guidance to agencies set forth in Office of Management and Budget Circular No. A-130 reflects that effort. Hence, agencies are already using the NII to widely disseminate economic statistics, electronic bulletin boards to advertise Federal contracting opportunities, and the World Wide Web to disseminate all types of information pertaining to their operations.

Another important and very successful public service use of the NII is electronic payments through electronic fund transfers (EFT). In Fiscal Year 1995, the Department of Treasury's Financial Management Service (FMS) delivered over 840 million payments worth \$1.3 trillion to the public. During that same period, FMS employed 15,000 financial institutions to collect \$1.4 trillion in corporate and individual income taxes, customs duties, Federal fines, and other levies.

Since its inception over 20 years ago, the Federal government has increasingly relied on EFT (or "Direct Deposit") to conduct many of these transactions. In fact, one of the Treasury Department's strategic business goals is that all of its payments will be done electronically by the year 2005. It is now commonly accepted that EFT is more reliable and more cost-effective than payment by paper check. Because payments are made directly to an individual account in a financial institution, recipients do not have to cash their checks upon receipt to use their money. Beneficiaries thus receive their payments safely, faster and, through the use of automated teller machines, have convenient access to them. The Federal government also comes out ahead, reaping the savings of the lower transaction costs of EFT. Also, because theft and forgery is reduced, the Federal government needs fewer resources for investigations, funds recovery, and payment reissue.

Current and envisioned electronic benefit delivery systems use either "swipe" or "smart" cards and some unique identifier, such as a personal identification number (PIN), to control access to benefits. Although these techniques have proven relatively secure to date, EBT is not without risk. The banking industry's experience with automated teller machines is illustrative. Cards can be lost or stolen, and PINs extorted using force. Cards can be counterfeited or manipulated to allow unauthorized access to funds. Information obtained electronically during a purchase can be misused by the retailer or other parties. The EBT Task Force is working closely with both the public and private sector authorities to effectively counter such abuses. Finally, broader use of EFT and EBT to distribute benefits will require creation of some form of a "bank account" to the 20 to 30 million Americans that currently lack this access.

The EFT and EBT programs continue to serve as laboratories for improving reliability and safeguards in the NII generally. As this Subcommittee heard from witnesses at its previous hearing on this topic in July, a number of products already provide electronic cash on the NII. One witness in particular, Dr. David Chaum, Chairman and CEO of DigiCash, Inc., described the counterfeiting of e-cash as presenting the same degree of challenge as the breaking of codes that were used to protect military secrets. Other witnesses discussed encryption and digital signature technologies as integral to their services. I will have more to say about of encryption in a moment, but first I want to briefly mention use of the NII for intragovernmental operations.

The use of the NII to support the internal operations of the Federal government presents additional challenges. During the conduct of regular business, agencies process a considerable volume of data -- some not so sensitive, some very sensitive, even classified information. For the most part, our needs are not so different from those of the private sector, and we expect to rely on the use of commercially available products to safeguard it. Predecisional discussions taking place via electronic mail or the transmission of personnel information within the government are not very different from corporate confidential strategic planning discussions via electronic mail or an employer's personnel files. However, as the sensitivity of the information increases, the reliance on the NII for the processing and transmission of such information introduces risks that require special safeguards. And as we move toward classified national security information, the importance of confidentiality increases. This then is the segue to a discussion of cryptography.

3. Cryptography

At the heart of security in the NII is the technical ability to protect information and the systems that process it. Often such techniques will depend on cryptography. Cryptography has a unique trait: it bonds its protection directly to the information being protected, thereby securing the information regardless of whether access to it is compromised. In an open environment, such as the NII, this trait is invaluable because it will often be difficult to control the location of and/or electronic access to information. The banking community has been a significant user of strong cryptography to protect its transactions for a long time, and will be for the foreseeable future. Indeed, as the witnesses at the July hearing pointed out, cryptography is an enabling technology for secure financial transactions, including digital cash in the future, protecting both the confidentiality as well as the integrity of the information.

At the same time, cryptography can thwart law enforcement's legitimate ability to understand the contents of information obtained by either lawful wiretaps or court-authorized searches and seizures. A number of years ago, we as a society decided that, for public safety reasons, our law enforcement agencies must have the ability, under tightly controlled procedures, to intercept certain electronic communications or seize property such as stored data. What could occur, however, with widespread use of strong cryptography to promote security on the NII, would be the inability of law enforcement to decipher what it legitimately obtained -- in effect allowing an individual to pre-empt these important public safety capabilities.

The Administration has proposed an approach to resolve this conflict known as key escrow. Under this approach, which is already being discussed with the private sector, keys to strong encryption are escrowed with a trusted entity. The keys would be provided to law enforcement authorities upon presentation of a duly executed warrant. This approach could also assist firms in recovering lost data, where, for example, a key has been lost.

Those who have followed this area will have detected an important change in how we are formulating our policy, particularly with respect to export controls. Initially the government developed and adopted the "Clipper Chip" to provide very secure encryption for voice telephone communications, while preserving the ability for law enforcement and national security. Industry representatives and privacy advocates raised concerns about some of the features of the Clipper Chip, and we began an effort to work with the public to design a more versatile, less expensive system for computer communications. Such a key escrow system would be implementable in software or hardware, would not rely upon a classified algorithm, would be voluntary, would permit the use of private sector key escrow agents, and would be exportable. As Mr. Kammer explains in his statement, we are attempting to engage all the stakeholders in developing an approach that truly balances the various interests.

It is important that we as a society have an informed dialogue about this important subject, and reach consensus on how to best resolve it. A balance must be struck between the public safety and national security implications of strong cryptography, and privacy concerns and the need for business confidentiality of our citizens and businesses in an international marketplace.

Closing

In closing, let me say that the technology of the future NII holds much promise -- we are still in the early stages of the information revolution, yet it is already changing our lives on a daily basis. The security and welfare of our children and grandchildren in the information economy of the future depend in no small part on how well we design and build effective security into the NII of today. Success in this endeavor will require cooperation and partnership among all interested parties in the public and private sectors. Together we can help realize the vision of a secure NII.

Thank you for your attention. I would be happy to answer any questions that you may have.



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

FOR IMMEDIATE RELEASE
June 14, 1995

CONTACT:
Lawrence J. Haas
(202) 395-7254

**NATIONAL INFORMATION INFRASTRUCTURE SECURITY ISSUES FORUM
RELEASES "NII SECURITY: THE FEDERAL ROLE"**

The Information Infrastructure Task Force's (IITF) National Information Infrastructure Security Issues Forum today released for public comment a draft report, "NII Security: The Federal Role."

The draft report summarizes the Forum's findings concerning security needs in the National Information Infrastructure (NII); presents an analysis of the institutional, legal, and technical issues surrounding security in the NII; and proposes Federal actions to address these issues.

"This report demonstrates the Administration's commitment to engaging the private sector and members of the public in a dialogue to ensure that the information superhighway is trustworthy and reliable," said Sally Katzen, Administrator of OMB's Office of Information and Regulatory Affairs. "We have worked hard to strike the appropriate balance between the Federal role as protector of the public interest and the private sector roles as owners and operators of the NII."

Contrary to news stories, the draft report does not propose to create new agencies to carry out Federal responsibilities. Rather, it is meant to stimulate a dialogue on how the Federal government should cooperate with other levels of government and the private sector to ensure that participants can trust the information superhighway.

To articulate and implement the Administration's vision for the NII, Vice President Gore formed the IITF, chaired by Commerce Secretary Ronald Brown. The NII Security Issues Forum was established within the IITF to address the important issue of security in the NII.

To better understand what will be needed to make the NII secure enough, the Forum and members of the U.S. Advisory Council on the NII held seven public meetings with government officials and members of the private and public sectors to discuss NII security needs. Today's release will continue this dialogue.

-more-

Electronic copies of the report may be obtained through the IITF bulletin board at iitf.doc.gov through both the Internet and the World-Wide Web. Dial-up access by modem is also available at 202-482-1920. Modem communications parameters should be set at no parity, 8 data bits, and one stop (N, 8, 1). Hard copies of the report may be obtained by contacting OMB's Publications Office at (202) 395-7332.

Comments are requested by September 19, 1995 and may be submitted to OMB, 725 17th Street, NW, Room 10236, Washington, D.C. 20503, to the attention of Virginia Huth or to huth_v@al.eop.gov.

#

NII SECURITY: THE FEDERAL ROLE

June 5, 1995

I. INTRODUCTION

The National Information Infrastructure (NII) is a system of high-speed telecommunications networks, databases, and advanced computer systems that will make electronic information widely available and accessible. The NII is being designed, built, owned, operated, and used by the private sector. In addition, the government is a significant user of the NII. The NII includes the Internet, the public switched network, and cable, wireless, and satellite communications. It includes public and private networks. As these networks become more interconnected, individuals, organizations, and governments will use the NII to engage in multimedia communications, buy and sell goods electronically, share information holdings, and receive government services and benefits.

Security is critical to the development and operation of a viable NII. In fact, one of the goals stated in "The National Information Infrastructure: Agenda for Action," is to ensure information security and network reliability. Without the confidence that information will go where and when it is supposed to go, and nowhere else, the NII will not be used to support health, education, commerce, public services, and advanced communications to the fullest extent. In the NII, security¹ means:

- . integrity -- assuring that information will not be accidentally or maliciously altered or destroyed;
- . reliability -- assuring that systems will perform consistently and at an acceptable level of quality; and
- . availability -- assuring that information and communications services will be ready for use when expected.
- . confidentiality -- assuring that information will be kept secret, with access limited to appropriate persons;

To articulate and implement the Administration's vision for the NII, the Vice President formed the Information Infrastructure

¹ The discussion of security in this report encompasses a number of substantive issues which are tangential to security, such as protecting intellectual property rights. The report does not attempt to set the underlying norms for these areas, but rather discusses protection of such information.

Task Force (IITF). The IITF is chaired by Secretary of Commerce Ron Brown and is comprised of senior Administration officials having expertise in technical, legal, and policy areas pertinent to the NII. The NII Security Issues Forum was established within the IITF to address the important cross-cutting issue of security in the NII. The Forum is chaired by Sally Katzen, the Administrator of the Office of Information and Regulatory Affairs in the Office of Management and Budget, and includes representatives from each of the IITF's committees as well as representatives from each Executive branch organization with significant information security responsibilities.

In addition to the IITF, the President has established the U.S. Advisory Council on the National Information Infrastructure. The Advisory Council includes representatives from industry, labor, State and local governments, and public interest groups, and advises the Secretary of Commerce on issues relating to the NII. Mega-Project III, one of three work groups of the Advisory Council, is addressing security, intellectual property, and privacy issues as they relate to the NII.

To better understand what will be needed to make the NII adequately secure, the NII Security Issues Forum and members of the U.S. Advisory Council on the NII held seven public meetings to discuss the security needs of likely users of the NII. Based on the first several meetings, the Forum proposed a set of five security tenets (set forth below) for public comment, which characterize in layman's terms the security needs of users of the NII.²

The purpose of this report is to expand on those tenets and begin to articulate security expectations for the NII in order to develop a broad consensus of the appropriate Federal role. Specifically, this report:

- Summarizes the Forum's findings concerning security needs in the NII;
- Presents an analysis of the institutional, legal, and technical issues surrounding security of the NII; and
- Proposes Federal actions to address these issues.

PUBLIC PARTICIPATION

² Although Mega-Project III co-sponsored the public meetings, this draft report is the product of the NII Security Issues Forum, a Federal organization. The Forum looks forward to receiving advice about this report from Mega-Project III through the NII Advisory Council.

Over the past year, the Forum, in cooperation with Mega-Project III of the U.S. Advisory Council on the National Information Infrastructure, conducted seven public meetings between government officials and members of the private and public interest sectors.

A general meeting was held on July 15, 1994, at which individuals representing business, manufacturing, banking, health, entertainment, publishing, education, libraries, and government services discussed their views of security needs in the NII. Subsequent meetings addressed the needs of various sectors using the NII. The subjects of the meetings were:

- (1) "Commercial Security on the NII," which focused on the need for intellectual property rights protection in the entertainment, software, and computer industries;
- (2) "Security of Insurance and Financial Information";
- (3) "Security of Health and Education Information";
- (4) "Security of the Electronic Delivery of Government Services and Information";
- (5) "Security for Intelligent Transportation Systems and Trade Information"; and
- (6) "The NII: Will It Be There When You Need It?" addressing the availability and reliability of the Internet, the public switched network, and cable, wireless, and satellite communications services.

In order to continue and expand this public dialogue, this draft report, "NII Security: The Federal Role," is being issued for public comment. In addition to receiving comments, the Forum will sponsor two public meetings this Summer to discuss the Report.

This report includes a set of proposed government action items in section IV. This is intended to articulate the areas in which the government will act to improve the security of the NII. The next step is to receive and respond to public comment on the report in order to develop consensus regarding the Federal role and its proposed actions.

II. FINDINGS

Based on the initial dialogue, the Forum is proposing three actions: (1) adoption of proposed NII Security Tenets, (2)

adoption of Organization of Economic Cooperation and Development (OECD) Security Principles for use on the NII, and (3) implementation of the Federal role described at the end of this report.

A. SECURITY TENETS

On February 10, 1995 [see Vol. 60 No. 28 of the Federal Register, p. 8100], the IITF proposed five security tenets for public comment, based on the general proposition that people who use the NII want to know that their information goes where and when they want it to and nowhere else. The tenets are comprised of five common propositions that emerged from the early public meetings about what NII participants expect. Clearly, the details of implementation of the tenets will vary by user -- whether teachers, doctors, or tax preparers -- and by application -- whether communicating over a two-way multi-media conference, sharing data between doctors and patients, or calculating a tax return. Participants expect:

- 1) The ability to control who sees (or cannot see) their information and under what terms.
- 2) The ability to know who they are communicating with.
- 3) The ability to know that information stored or transmitted is unaltered.
- 4) The ability to know when information and communication services will (or will not be) available.
- 5) The ability to block unwanted information or intrusions.

Two conditions attach to these security tenets:

- 1) None of these tenets is absolute. For each tenet there may be valid societal reasons -- such as an emergency or a need to protect another's rights -- that cause the tenet to be conditioned in some manner.
- 2) Each tenet requires NII participants to take responsibility for establishing the terms and conditions under which they will exchange information. The distributed and empowering nature of this technology demands a greater level of personal responsibility from participants than when communications systems were more limited in scope and scale. Education of NII participants is thus a critical task.

B. OECD PRINCIPLES

The U.S. is not alone in addressing security concerns in the evolving global information infrastructure. The organization for Economic Cooperation and Development (OECD) has adopted Security Guidelines. The U.S. and 23 other member nations of the OECD have endorsed these Guidelines. The Guidelines encompass nine Security Principles, which articulate high-level needs, such as the need for explicit accountability for security, the need for awareness of security practices and procedures, and the need to respect the rights and legitimate interests of other users. These Principles are included as Appendix A. The IITF proposes to adopt those Principles for use in the NII.

The OECD Principles are being incorporated into two National Institute of Standards and Technology (NIST) publications, "An Introduction to Computer Security: The NIST Handbook," and "Federal Computer Security Principles and Practices" (working title). These two publications complement each other -- the Principles and Practices publication will provide a quick reference to accepted security practices. The Handbook explains the Principles and Practices and provides a bibliography and extended examples.

C. PROVIDER AND USER SECURITY CONCERNS

The public meetings solicited discussion with a broad range of NII participants, both users and providers of NII services. Regardless of the commercial, industrial, or public interest use represented, the participants shared a number of concerns. These concerns included: the potential inability to control secondary uses of information; questions of liability for loss or inappropriate access to or use of information; a mistrust of government's use of information; the desire to protect one's own system from outsiders, whether by hostile attacks or junk mail; and risk of system failure at times of critical need. The most-heard concern was that personal information, such as information pertaining to an individual's finances, health, or purchasing habits, could be disclosed to or manipulated by an unauthorized user. These shared concerns were generalized in developing the security tenets described above.

In addition, some participants seemed to desire a greater government role, such as censorship of defamatory or pornographic information transmitted over the NII, or additional funding for national security and emergency preparedness programs. Other participants seemed to desire a lesser government role. For example, some participants desired open access to and use of virtually all information and systems without interference. Other participants criticized the Federal government's export control policy, which limits the export of powerful cryptographic systems.

Still others were suspicious of the technology underlying the NII and how it would be used. Some witnesses were also concerned that government's involvement could create greater inefficiencies, increase susceptibility to invasions of privacy and risk of fraud, and contribute to the depersonalization of society.

The following summarize the concerns and needs heard at each of the public meetings. Transcripts are available on the NII bulletin board at the Department of Commerce. (For Internet access, gopher, telnet, or anonymous ftp to iitf.doc.gov. Access is also available over the World-Wide Web. Dial-up access by modem is available at (202) 501-1920. Set parameters at no parity, 8 data bits, and one stop. Speeds of up to 14,400 baud are supported.)

1. Entertainment, Software, and Computer Services

Images, movies, music, software, and a variety of products that can be transmitted in digital form can be easily altered or copied. The protection of intellectual property rights in an electronic age requires technology, legal protection, and institutions that promote fair use, support licensing and payment, and prevent unauthorized copying, alteration, or distribution. There was considerable discussion about effective legal protection and institutions. A thorough treatment of intellectual property on the NII will be found in the IITF White Paper.³

A number of possible technological approaches were described at the meeting, including software that is programmed to be disabled after a span of time if the software is not paid for. Another technique described was to distribute an encrypted movie with a key that can decrypt it (for viewing) one time only. One intellectual property entrepreneur electronically distributed his work -- visual images -- in encrypted form and then sold the decryption key through the regular mail. This solution allowed him to distribute digital images electronically, but it did not prevent the buyer from redistributing the work after they decrypted it. Generally, participants indicated that adequate technical capability was being developed to protect their own products. Technical challenges remain, however, including the need for an automated copyright management system for digital works. In addition, several witnesses raised a concern about government barriers to the development and sale of technologies such as export control laws.

³ The report is expected to be issued in June, 1995. For a copy of the report, contact the U.S. Patent and Trademark Office, Washington, D.C. 20231, or call (703) 305-9300.

2. Health and Education Information and Services

Health care will be improved by computer-based patient records, on-line databases, consumer health information, and remote treatment and advice. However, improved access to information also brings with it a risk of improper disclosure, alteration, or use of highly personal information. Patients' well-being will become dependent on the integrity and reliability of such information in the NII. In particular, the reliability of such computerized medical records systems will be of critical importance as the health care system shifts away from paper. Similarly, educational records can have a substantial effect on individuals' economic well-being.

Participants suggested that the technology will need to promote information integrity, and to ensure that access is provided on a need to know basis, that records that serve different functions are separated, and that the records are destroyed when they no longer serve their function. Concern was also raised about the availability of pornographic material on the Internet and the need to protect children from exposure to it.

3. Financial, Insurance, and Commercial Services

The financial and insurance sectors have relied for decades on closed networks in order to reliably transfer funds and share information. As their networks become more open, new security tools and techniques will be needed to protect the confidentiality and integrity of valuable commercial information. Questions of liability will also arise if improper disclosure of customer information occurs while it is being transmitted over the public switched network.

As consumers use the NII to conduct business, they will want to verify that a payment or order was received correctly. Without a face-to-face transaction to verify the authenticity of the customer and of the vendor, the potential for fraud increases for both parties, requiring methods of electronic notarization, digital signatures, and date-stamping.

The advent of so-called digital cash involves a different challenge. It requires a technical method to avoid forgery and authenticate the current owner. On the other hand, some witnesses favored the ability to anonymously execute transactions. A number of products are already being tested to provide "electronic cash" on the NII.

One witness pointed out that the vast majority of technical solutions address the issue of protecting an organization's data

from individuals, while little attention has been paid to the problem of how the individual's data can be protected from organizations. This situation is illustrated by the way in which data about an individual's purchasing habits is bought and sold in private markets. Other personal information which is generally publicly available, such as marital status, home ownership, and status in legal proceedings, is collected by the private sector and sold as a commodity. Some individuals expressed a desire to exercise greater control over the use of this information, or to be reimbursed for its use. The IITF's Privacy Working Group is developing principles to guide policy development in this area.⁴

4. Intelligent Transportation

Intelligent transportation systems include applications such as electronic toll collection, in which a toll payment is automatically deducted from a card with a computer chip so that cars won't have to stop as they pass through toll booths. Such systems may also help monitor traffic patterns and road conditions through cameras or other sensors, and provide drivers with information in their cars about the quickest route.

A basic security concern with electronic toll collection is funds control and integrity. In addition, there are concerns that the information collected in these transactions, including information about the owner of the vehicle, how fast he or she was driving, and where he or she was headed, could be used inappropriately. Access to this information could disclose commercial proprietary information or compromise personal privacy. Furthermore, as transportation becomes more dependent on automated control systems, the movement of people becomes subject to security risks. For example, a security breach could allow mischief such as switching all the traffic lights to green, thus promoting accidents.

5. Government Information and Services

Use of the NII is becoming integral to virtually every Federal program, and Federal agencies are becoming dependent upon that use for execution of their missions. The NII will support programs as varied as air traffic control, compilation of the decennial census, response to natural disasters, and delivery of social security benefits.

⁴ "National Information Infrastructure; Draft Principles for Providing and Using Personal Information and Commentary;" January 20, 1995; 60 FR 4362.

This use of the NII in Federal operations promises improved efficiency of governmental program delivery. However, it also introduces new and varied security vulnerabilities, not unlike those faced by other users of the NII. The difference, of course, is that addressing these security vulnerabilities is a direct responsibility of the Federal government, since such vulnerabilities could degrade Federal program effectiveness and resource safeguards, and affect the integrity, confidentiality, and/or availability of government information.

At the meeting, the use of "smart cards" or electronic debit cards for delivering food stamps was discussed in depth. Smart cards provide the advantage of on-time payment, increased dignity, and improved efficiency in program administration. However, cards can be lost, and there are opportunities for fraud by converting the credits to cash. Other concerns include the potential for counterfeiting such cards or otherwise manipulating the value of the cards. Unauthorized access to individual purchasing records could violate personal privacy. Users of these cards need confidence that the benefits will be available when they expect them to be, and that associated information will not be abused by those with access to it.

6. The Public Switched Network and the Internet

As new technologies are integrated into the public network, new vulnerabilities are introduced. Some technologies are more vulnerable than others. For example, wireless communications are particularly vulnerable to eavesdropping, while cable and satellite television providers face an ongoing battle to protect the commercial information they are sending to consumers.

As individuals and organizations become more reliant on the NII to conduct personal and business transactions, the availability and reliability of the network is of greater importance. These concerns vary from the risk of major network outages to the minor irritant of slow or noisy network connections. Users need assurances that the NII will be there when they need it. If it isn't, they want meaningful recourse. For certain transactions, users also desire an assurance that information was received by the intended recipient, analogous to "certified mail."

Users will depend not just on the availability and reliability of the information itself and of the system on which it resides, but indirectly on the availability and reliability of the network which transports the information between systems. From the perspective of the providers of network services, security threats include natural disasters such as fires, floods, or hurricanes; physical attacks, such as bombs; electronic attacks, such as computer viruses; and unintentional errors, such

as design flaws, software bugs, and human error. Network services providers are addressing these threats as an integral part of their business. During the public meetings, some participants were open to appropriate Federal involvement in this area, while others were more cautious about the Federal role in this area.

Other concerns include the risk that hackers may intentionally compromise the security of personal or organizational computer systems, or maliciously gain access to information while it is moving from place to place within the NII. These fears are grounded in well-publicized incidents on the Internet and public switched network, but actually comprise only a small fraction of computer security incidents. The majority of incidents are caused by authorized individuals doing unauthorized activities. There was some discussion of the need to share information among providers concerning the outside threats to networks, as well. Other security concerns included the need to verify whether information was altered accidentally and the need to ensure availability of networks in the event of natural disasters.

III. ANALYSIS

The NII security needs expressed above can be organized into three areas: (1) coordinating functions, (2) oversight and enforcement for public safety, and (3) technical security needs. The three areas are interrelated. For example, for Federal computer crime law to be enforceable against a system trespasser, security measures must have been in place and a record made of the trespass. Similarly, civil liability standards of due care require that effective technical security be in place. At the same time, overall security is enhanced if there are criminal or civil legal sanctions which act as deterrents.

The following section addresses the functions necessary to support a secure NII, as heard in the public meetings. The section on oversight and enforcement for public safety addresses how existing oversight organizations need to adapt to the oversight of NII related activities, as well as whether current laws are sufficient and enforceable in the context of the NII. The discussion on technical security addresses the technical ability to protect information and systems in the NII.

A. COORDINATING FUNCTIONS

The National Research Council's (NRC) report, "Realizing the Information Future," notes that while security needs can be addressed to some extent by technological methods and a legal framework, structures must be in place to make them work. This

section is intended in part to contribute to the dialogue about and development of such an architecture, by describing the coordinating functions which emerged based on public discussions of security of the NII. Some of these functions will be fulfilled by the private sector, some by government, and others in partnership.

If the NII is to succeed, a structure or a collection of structures -- a security architecture -- must exist to ensure security. The NRC report states: "This security architecture must include technical facilities, recommended operational procedures, and means for recourse within the legal system." This architecture will be based on a variety of public and private institutions and policies. Although an architecture will define how institutions, policies, and technologies interconnect, a sound security architecture will consist not of rigidly prescribed technologies or solutions, but must be able to flexibly adapt to change. The report also notes that such an architecture will require research and development over time.

1. National and Economic Security

As the United States as a whole becomes increasingly reliant on the NII for communications and information, other key components of the U.S. infrastructure will become dependent on it. For example, the power grid, transportation systems, financial institutions, and economic transaction data will all be dependent on the NII. Security weaknesses in the NII can place those infrastructure elements at risk. Hence a significant attack on the NII would be a threat to our national security in addition to the significant personal and economic harm it would cause.

From the Federal government's perspective, public safety and the national defense call for a secure NII. All Federal entities that oversee various parts of the U.S. economic infrastructure must be aware of the changing risk that increasing reliance on the NII entails. They also must be aware of the various types of threats to the NII and their magnitude.

2. Ethics and Education

There was a general concern at the public meetings about the lack of regard that many participants in today's Internet had for others' intellectual property and privacy. This was often characterized as youth in its search for knowledge and disdain for bounds of ownership of electronic information. Several presenters noted that often young persons have tremendous technological savvy, but little understanding of the ethical responsibilities that such knowledge entails.

Witnesses at the public meetings specifically suggested a need for training and awareness in the general area of computer ethics. The basic principle should be a respect for others' rights on the NII. Whether in the office, university, elementary school, or at home -- where today's children are learning to use computers -- parents, teachers and supervisors should emphasize that it is not only wrong, but illegal, to copy copyrighted software or other materials or to break into someone else's file or computer system. It was noted that the Education Department, in cooperation with the Intellectual Property Rights Working Group of the IITF, has begun to develop a model curriculum on the importance of protecting intellectual property. Participants at several meetings described the need for ongoing dialogue on this subject among all users.

A final issue where more dialogue is needed is the protection of children from exposure to inappropriate materials on the NII. As President Clinton has stated:

"I believe that insofar as governments have the legal right to regulate obscenity that has not been classified as speech under the First Amendment, and insofar as the American public widely supports, for example, limiting access of children to pornographic magazines, I think it is folly to think that we should sit idly by when a child who is a computer whiz may be exposed to things on that computer, which in some ways are more powerful, more raw and more inappropriate than those things from which we protect them when they walk into a 7-Eleven."⁵

3. Emergency Preparedness and Response

Three types of emergency preparedness and response roles were described during various meetings: (a) the need for an entity analogous to the Computer Emergency Response Team (CERT), which currently acts as an Internet "911," (b) a system for planning and recovery during and after an emergency which sets, among other things, a priority of restoration, and (c) a need to exchange information concerning mutual vulnerabilities.

(a) Emergency response. As the Internet is evolving from a research and development experiment to a widely used public communications medium, the need for an emergency response entity to coordinate the community's response to security threats has become apparent. In the Internet the entity that currently performs that function is the Computer Emergency Response Team (CERT). It is likely that function will need to continue in the

⁵ Remarks to the American Society of Newspaper Editors, Dallas, Texas, April 7, 1995.

NII.

(b) Emergency planning and recovery. In order to maintain a state of readiness or respond to and manage an emergency or crisis, an emergency preparedness capability is required. The government has established the National Communications System (NCS) to ensure the availability of communications services required to support emergency planning and response functions. The NCS's National Coordinating Center for Telecommunications is staffed full-time by both government and telecommunications industry representatives, whose mission is to respond to both military and civil emergencies, e.g., Operations Desert Shield/Desert Storm, Hurricane Andrew, the Northridge earthquake, and more recently, the bombing of the Federal building in Oklahoma City. A similar function is likely to be needed to ensure the availability of NII services to support emergency planning and response functions.

All users have an interest in having service restored in the event of an emergency or disaster such as an earthquake or flood. In the public switched network, telephone service is restored based upon governmentally established priorities, with the highest priority given to organizations whose function it is to respond to such emergencies, such as the Federal Emergency Management Agency (FEMA). As users rely more on the NII for critical functions, a similar need for setting priorities for restoration on a broader level will arise.

(c) Exchanging information concerning vulnerabilities. Participants at several meetings discussed the need to exchange information about mutual vulnerabilities in the NII as it evolves. They indicated that improved security resulted from meaningful communications among users and providers. If a problem is identified, it can be quickly solved. In describing this role, some pointed to CERT bulletins as a model. Others pointed to the NCS's program to facilitate appropriate sharing of security vulnerability information. Others described different possible mechanisms, such as industry newsletters and trade publications, engaging in mutual assistance agreements with other parties in the private sector, and on-line news groups.

4. Quality Assurance

Some participants in the public meetings asked how they could be sure that the security products they chose were as good as they claimed to be. Testing by independent third parties such as nationally recognized testing laboratories, organizations that certify that products meet or exceed the requirements of a specific standard, may be useful for those trying to evaluate the effectiveness of security products. Such third party testers may evolve into a system for evaluating security products. A

certification procedure could be useful for both producers and users of security products who may be trying to be more competitive and to protect against the threat of lawsuits. Utilization of the trademark system may also operate to provide assurance of performance. The trademark system may be useful in allowing consumers to develop confidence in a particular trademark that could result in continued purchase of both a particular product and of others bearing the same trademark.

Additionally, an independent entity representing consumers' interests such as a "Better Business Bureau" could provide a place to file complaints and answer questions about various NII service providers. Either government, trade associations, industry groups, or private sector consultants could fulfill this need.

Related to the issue of accreditation is that of standards. Security products and services can be tested as meeting either a performance standard or a technical standard. Standards in the United States are developed primarily by private standards development organizations representing industry, trade, and professional organizations. For example, the American National Standards Institute (ANSI), the Institute for Electrical Engineering and Electronics (IEEE), and others are active in this area. Sometimes a Federal government standard becomes the accepted international standard. Many of these organizations work together through the International Standards Organization (ISO). Internet standards have been developed somewhat more informally and quickly by the Internet Engineering Task Force (IETF).

Alternatively, any group of users can define a set of security standards and agree among themselves to be bound by them. Such "affinity groups" design or decide on standards to meet the specific needs of their members. During the public meetings, participants described unique problems such as the need for a particular database to increase the integrity of information, or to help their industry improve its use of electronic processing and networking. These standards may become de jure standards formally accepted by industry, or they may remain de facto standards. In addition, de facto standards are often set by dominant industry participants. Quality assurance and other security standards must be developed in full recognition of the complex standards-setting environment.

B. OVERSIGHT AND ENFORCEMENT

There is a need for effective law and oversight of both the NII itself and of public safety-related uses of the NII. A sound legal system that applies civil remedies and criminal penalties is essential to fulfilling this need. In the public meetings,

participants focused primarily on civil remedies and litigation, rather than criminal issues. In addition, considerable activity is occurring in State, local, and Tribal governments, particularly regarding criminal computer law.

1. Law and Regulation

Various activities are overseen by government because they affect the well-being of the nation. For example, some sectors of the economy are regulated to ensure the public health or safety. As these activities become increasingly reliant upon the NII for communications and information, a security weakness in the NII can become a threat to the public health or safety. To effectively manage risk in their public safety oversight role, Federal agencies will need to ensure the secure use of the NII by their overseen sector. Thus, for example, the Transportation Department may need to adjust its regulatory oversight of aircraft to account for the risks involved in aircraft's use of the NII. Similarly, the Securities and Exchange Commission may need to adapt its oversight of securities exchanges, and the Treasury Department and the Federal Reserve Board their oversight of the nation's banking system.

2. Civil Law

Civil litigation includes specialized or statutory suits, contract actions, tort actions, and injunctive relief. Several participants in the meetings stated that issues of liability must be resolved before widespread use of the NII occurs. In reality, however, a range of accepted solutions and practices concerning information security will be decided in increments through the court system as a body of case law develops over time.

Civil law addresses the issue of liability. In every public meeting, users and providers of NII services questioned how the current system of liability for damages would affect their use. For instance, concerns were raised that unknown exposure to liability could prevent potential providers from offering services.

Specialized suits can be used to protect intellectual property rights against copyright, patent and trademark infringement, or other violations of established statutory rights. Whether a particular statute extends to activities on the NII when Congress did not specify the statute's application in a networked environment may be subject to litigation on a case-by-case basis.

Contract actions are law suits contesting provisions in express or implied contracts. Tort actions resolve disputes for

money damages alleging a breach of a duty which caused harm to the plaintiff. Injunctions involve obtaining a court order to prevent specific actions or require certain activities. For example, such an order might prohibit use of the Internet in a certain way or require a user to make certain disclosures before using the Internet. Other forms of civil action and novel theories of liability involving all aspects of the NII continue to evolve.

Civil liability is likely to create incentives for improving security of information systems.⁶ If users, system managers, and service providers face liability in contract for failure to perform a contractual duty, or liability in tort for negligence, they will have an incentive to take reasonable steps to secure their systems, ensure accuracy of their data, and limit unauthorized access and use. A presenter at one public meeting noted that some private parties currently protect their proprietary information by simply not putting it on networks. Attaching legal consequences for the unauthorized or improper use of electronic data will increase the likelihood that the NII will be a trustworthy, reliable system.

Courts are beginning to be confronted with cases that test the effects that civil liability practices will have on the security of the NII. Until a settled body of law develops, various parties' responsibilities and potential liability for negligent security will be uncertain. Legislation that would impose criminal and/or civil penalties for security violations such as blocking, tampering, masquerading, or denying service in the network environment is, of course, possible. However, consensus about what constitute reasonable standards for information security will be difficult to achieve. Because security requirements greatly vary in different contexts, such as finance, law enforcement, medicine, national security, research, and education, there may be a need for context-specific standards that can evolve as requirements change.

3. Criminal Law

Traditionally, laws have focused explicitly on the computer, since it could be easily recognized as the venue where a crime occurred. The laws were intended to protect the information

⁶ Lost or scrambled files, system downtime, invasion of privacy, and economic or physical injury can be foreseen as a result of sloppy security of networks. For example, liability for system managers can be envisioned for failure to enforce password expiration, eliminate access by former employees, replace default configurations, or implement technical solutions to prevent or reduce breaches in security.

contained in computers. Technology, however, has evolved so that proscribing conduct with regard to computers does not adequately protect information. Today, information can be intercepted and modified in transit between computers, or when it is present in devices not typically thought of as computers, such as telephones, cable systems, satellite and cellular channels, etc.

Many actions that would compromise security of the NII are already criminal violations. For example, it is illegal to conduct a wiretap without a court order. Fraud, whether perpetrated electronically or not, is a criminal offense. In other areas, laws may need to be amended.

Legislative efforts to protect computers and information suffer, on the one hand, from having to exhaustively yet clearly define these terms in order to make the laws meaningful. On the other hand, the laws must be sufficiently broad and adaptable that the statute will not be rendered obsolete by rapid technological change. For example, current law may not deal well with the problem of intrusive code, also known as a computer virus or worm. That is, it may be difficult to prosecute the distributor of these destructive instructions if that individual never actually "accessed or used" the affected computer.

Although existing laws provide some protection, new laws will be needed to insure that the NII is protected adequately. For example, 18 U.S.C. Sec. 1030(a)(5) should be extended to protect all United States Government and financial institution computers, even if the computer is not used in interstate commerce or communications. Additionally, the statute should specifically apply to computers used in foreign communications, not just interstate communications. These and other changes must be made to ensure that laws keep pace with new technologies.

In order for the NII to be secure, laws must be enforceable. Hence, law enforcement officials such as police officers must maintain the ability to enforce laws effectively in it. Future crimes are likely to be planned and coordinated using the NII. The NII will also be used by criminals to smuggle stolen corporate information, engage in the transmission of child pornography, engage in industrial sabotage, or electronically stalk, terrorize, or threaten other NII users. In all of these cases, law enforcement must be able to protect citizens.

4. International Issues

International computer offenses are easier to commit than traditional international crimes, because they do not necessarily require additional manpower or physical transportation. Someone can ship information covertly via telephone and data networks. They need no passport and pass no checkpoint, but cross borders.

simply by typing a command.

Second, computer crime has not received the emphasis given other international crimes. Until relatively recently the United States, probably the most computerized nation, has not mobilized against computer criminals, even though it is the frequent target of such computerized attacks. Although the U.S. now recognizes the seriousness of the threat, it is not surprising that less computerized countries do not yet fully share this awareness.

Many countries have weak or no laws against breaking into computers. Those with strong laws find it difficult to engage in fruitful cooperation with those without. The vulnerability of both modern and modernizing nations has been highlighted by recent events:

- A Christmas card message sent over BitNet, the international academic computer network, landed in 2,800 machines on five continents including IBM's internal network. It took only two hours for the benign virus to spread 500,000 infections worldwide, forcing IBM to take the network down for several hours to accomplish repairs.
- Pirate bulletin boards contain information regarding computer vulnerabilities and are being used to develop and perfect new computer viruses. Such bulletin boards have been found throughout the United States as well as in Bulgaria, Italy, Sweden, and the Soviet Union.
- In China, computer criminals recently stole \$235,000 from a bank in Chengdu.
- Recent reports indicate highly prolific virus writers are working in Bulgaria.

In order to improve international cooperation in the prosecution of computer crimes, the United States has joined international efforts to raise public consciousness about computer crime and encourage other countries to enact or strengthen their computer crime laws. In fact, other countries have been working both domestically and internationally in this area, particularly Denmark, England, Australia and Germany.

Consistent with this international effort, the Organization for Economic Cooperation and Development's Guidelines for the Security of Information Systems require prompt assistance by all parties in cases where information security has been breached. Additionally, the Council of Europe is currently addressing procedural problems that arise in information technology crimes, such as how to quickly get international trap and trace information.

C. TECHNOLOGY

At the heart of information security in the NII is the technical ability for individuals to protect their information and systems. At every security meeting technical approaches in use or being developed to protect systems or information were discussed. These varied from techniques being used by firms to protect their intellectual property rights, to protection being designed into systems of electronic cash, to "firewall" techniques for protecting firms' networks when connected to the Internet. These public discussions indicated that the marketplace, to the extent that users are demanding security, is responding with both specific security products as well as general NII products and services that incorporate security protection.

At the same time, the security technology challenges of the NII are formidable. Information and services will need to be protected, yet also available to communities of interest. Much of the technology that will be used to provide security in future use of the NII is yet to be developed. The discussion in this section that follows summarizes today's technological approaches to security, based on the public meetings. It should not be read as a complete description of the security technology needs of the future NII, nor to minimize the complexity of fulfilling those needs.

Security products and methods are necessary for individuals and organizations to be able to protect their systems and information in the NII. The many products and techniques that exist approach security from one of two principal strategies -- protecting a system from outside attack (e.g., firewalls), or protecting the information itself regardless of where it resides, normally through some form of cryptography. In addition, the networks themselves should be protected.

1. Protecting Systems

Like criminal laws, technical security measures have traditionally focused on controlling access to the system. As today's processing environment becomes more open, however, that task becomes significantly more difficult.

Participants in the public meetings demonstrated an understanding of a wide array of technical security techniques used to protect their systems. Moreover, a consensus view emerged that incentives exist for the marketplace to provide appropriate security techniques. A number of participants expressed surprise that the government was taking an interest in this issue, other than as a user. Most felt that their technical

security needs would be satisfactorily addressed by the private sector.

a. Access Control to Systems

Today, individual access to and accountability on systems is controlled largely by password management. That is, an individual is required to identify some unique piece of information known only to the individual and the system in order to identify himself to the system. Over the years, password schemes have become more complex to make systems more secure, and the ability of those trying to penetrate systems by obtaining passwords has become substantially better. For example, a large number of sophisticated password "sniffers" -- software programs designed to capture passwords as they are sent across hosts -- were recently detected on the Internet.

Stronger schemes for protecting systems include timed password-changing mechanisms. These mechanisms change acceptable passwords at timed intervals previously agreed upon between the system and a device held by individuals desiring to remotely access the network. Other methods are being developed to substitute for password schemes. They identify individuals to a system by the rhythm of their keystrokes or by biometrics such as fingerprints or a retinal scan.

b. Secure Gateways

Participants at the public meetings that use Internet noted that they were using secure gateways or "firewalls" to help protect their systems by limiting outside access to internal system capabilities. It was often noted at the meetings that, despite recent publicity about break-ins and breakdowns, strong technical measures exist that afford protection. Where break-ins have occurred, they normally exploit known weaknesses which have not been fixed, even though fixes are readily available.

A different concern raised by a number of participants at the public meetings is the need to block the reception of unwanted information. This can be a security risk because unwanted messages could overwhelm a receiver's ability to handle them and effectively shut down the receiver's system.

A view that was often presented was that individuals and organizations are responsible for making reasonable efforts to secure their systems, in the same way they have a responsibility to lock their doors to deter burglars from entering. Private sector firms are responding to the need for secure gateways by developing increasingly sophisticated commercial products. However, like seat belts in cars, they only work when they are

used.

c. Protecting Networks

Related to the security of systems is the security of networks. Networks, comprising a variety of technologies, are what connect systems with each other. The most common threats are breakdowns in the availability and reliability of the networks, resulting in slow or noisy connections, network outages, or loss of data. These threats can be caused by natural disasters such as fires, floods, or earthquakes, but also can include a physical attack, such as a bomb, or an electronic attack, such as a virus. Procedural errors such as design errors, software bugs, and operational mistakes can also place a network at risk.

Basic physical security precautions can help, such as fire protection systems and doors with locks. Back-up equipment enables a network provider to quickly restore service, while quality assurance software can minimize design errors, and technical security measures can warn about an impending breakdown or prevent an outage or loss of data.

2. Protecting Information

Protecting information requires different technology than protecting a system. Once information is outside a controlled system, there is little control over who can gain access to it. Therefore technology which can provide assurance that information itself can not be read, copied, or modified is critically important in an open processing environment such as the NII.

a. Cryptography

Cryptographic mechanisms already widely used are unique in that they directly protect information from being compromised or altered without authorization. It is envisioned that use of encryption and digital signatures will continue to grow rapidly. Cryptography is used by banks to assure the integrity of financial transactions, by computer operating systems to conceal passwords, by users of the Internet to protect the privacy and confidentiality of their communications, and by holders of smart cards to protect information contained on the card. There is no doubt that in the future there will be widespread use of this technology, which will be virtually transparent to end-users. Cryptography is also used in other security services, such as digital signatures and passwords.

Some participants noted that many hurdles remain to easy use

of cryptography. For example, one problem is the awkwardness of handling encrypted information. Also, the lack of a public key infrastructure makes it difficult for individuals and organizations to manage keys efficiently and to use public key cryptography. Another factor which has limited cryptography is the risk of unmanaged cryptography for business -- whether it be a disgruntled employee who encrypts corporate financial records before departing, an employee who is absent when critical files are needed, or merely someone who forgets the keys. Finally, the lack of agreement on cryptographic standards is slowing the proliferation of cryptography.

1. Confidentiality

Cryptography is essential to protecting the confidentiality of automated information. It provides the protection of information being undecipherable, even if someone gains access to it. It is this use that crystallizes a conflict between citizens' needs to protect confidential information and the societal need for justice and safety. Strong cryptography can be used to thwart law enforcement's legitimate ability to understand the contents of lawful wiretaps. On the other hand, weak cryptography will not provide effective protection of confidentiality of citizens' sensitive communications.

A number of alternative approaches to resolve this dilemma are being proposed. Many involve a key escrow approach whereby, keys to strong encryption are escrowed with a trusted entity. Under this approach, the keys would be provided to law enforcement authorities upon presentation of a duly-executed wiretap warrant. Some of these approaches could also assist firms in recovering lost data, where, for example, a key has been lost. Private sector approaches being developed to meet the needs of corporate key escrow may also benefit government, both as a user and in its law enforcement responsibilities.

As a user, government has its own needs for security. In order to protect its voice and low-speed telephonic data communications, the government has developed and fielded a technology to meet these needs, known as the Escrowed Encryption Standard, or "Clipper" chip. It is available for voluntary use by the private sector, but individuals may continue to choose to use any encryption technique domestically.

The private sector has reacted strongly to this initiative, objecting to the key escrow feature, to the fact that the technology is hardware-based, and to its use of a classified algorithm. However, this technology gives government no new authority or abilities. Instead, it enables government to protect its own information while supporting effective law enforcement.

2. Digital Signatures

In an open digital environment, verifying the source of a message or document and assuring that it has not been changed was mentioned as a concern in a number of different meetings. For example, in electronic payments there is concern that the correct payment is made to the correct individual. As noted at the meetings, the private sector is actively working on providing this capability and assuring effective protection. The underlying technology for such protection is digital signature.

A digital signature is created by applying an encryption algorithm to the information, resulting in a unique "signature" associated with the information. This signature is encrypted and sent with the information, which may or may not itself be encrypted. By verifying the signature and comparing it with the information, the receiver can verify that the contents of the message were not altered in transit. Of course, such a technique does not prevent or correct alterations, it only detects them.

While there are a number of different technical approaches to digital signatures, two are prevalent in the current environment. One, based on the RSA encryption algorithm, is coming into wide use in the private sector. A second, based on the El Gamal algorithm, has been adopted as the Federal standard for signature and is coming into use in the Federal government. Both require a public key infrastructure to provide a trusted third party, which will allow verification that the signer of a given document is indeed who he or she claims to be.

3. Public Key Infrastructure

In tomorrow's open networks, cryptography will help to verify the identity of a message sender, assure the integrity of a message, and protect information from unauthorized readers. Without some means of verifying where and to whom their information is going, people may hesitate to do business electronically. A Public Key Infrastructure (PKI) uses two keys, one public, like a phone number, and the other private, like a personal identification number (PIN) or password. The public key is listed in a public electronic directory, while the private key is kept secret by the individual.

The primary application of a PKI is to verify the identity of a message sender through creation of a digital signature. To create a digital signature, a sender of information uses her private key to sign the message. The receiver uses the sender's public key to verify the signature.

A PKI can also support confidentiality of messages. A sender of information obtains the receiver's public key and encrypts the data. The receiver uses his private key to decrypt

the information.

A public key infrastructure has great potential to encourage new activity on the NII because it provides a means to do business among parties without prior arrangements. For example, a mail order company posts its public key in an on-line catalogue. Customers send in their order with their credit card number in encrypted format. The company uses its private key to decrypt the information.

b. Protecting Against Copying

A more difficult technical problem that is being addressed by the private sector is protecting information against unauthorized copying. Technology using encryption to prevent data from being read by individuals who are not authorized to read it is readily available. However, preventing individuals from making unauthorized use of data they have been authorized to read is a more difficult technical problem to solve.

Once someone possesses a document in electronic form, it is easy to copy and redistribute it. If the information is copyrighted or protected by non-disclosure agreements, there is little more that the owner of the information can effectively do. Intellectual property owners are concerned that if they disseminate information with commercial value such as software, music, books, or video images, it will be widely pirated. Many of these property holders have traditionally disseminated in other media, such as paper or film.

Efforts to protect copyrighted software from unauthorized reproduction provide an interesting case study of the various approaches -- both legal and technical -- used to protect intellectual property rights. Some software developers have used cryptography to prevent illegal reproduction of their software. Alternatively, the Software Publishers Association (SPA) has a two-fold approach to this issue: it sues corporations that make illegal copies of copyrighted software, and it is also conducting a campaign to educate the public on software copyright issues. However, the international component of this problem makes legal and educational remedies difficult.

IV. GOVERNMENT ROLE AND RESPONSIBILITIES

The NII will be designed, built, owned, and operated by private citizens and private organizations. It will primarily be used by individuals and organizations, but it will also be used by Federal, State, local, and Tribal governments in support of their missions. The Federal government has an important role in the continued development and growth of the NII as a leader, facilitator, a promoter of the general welfare, a catalyst, and a

model user.

Based on information generated from the public meetings, the private sector is addressing many of the security needs of the NII. NII security, like other aspects of the NII, will be developed, built, and used by the private sector. Products and services that can be used to secure information on the NII will be designed and provided by the private sector in response to market demands. This section of the security report proposes the role of the Federal government in supporting a secure NII.

The Federal government will undertake four main activities for improving NII Security. The first three involve the government's responsibilities to ensure the sound development and use of the NII. The fourth is the government's responsibility as a user of the NII.

First, the Federal government will serve as a facilitator and a catalyst for promoting private sector activity.

Second, in its role as guardian of the public interest and general welfare, the Federal government will cooperate with other governments, the private sector, and the public-at-large in setting legal and policy ground rules for security in the NII.

Third, the Federal government can support the private sector's development of needed technology by funding research and development in critical areas.

Fourth, as a model user of the NII, the Federal government has a responsibility to ensure that its own automated information is secure.

A. As facilitator and catalyst for private sector activity, the Federal government will (1) adopt the NII Security Tenets and the OECD Security Principles for use on the NII; (2) stimulate dialogue and awareness about security risks, needs, and solutions; (3) make Federal security products and techniques available for use in the NII; and (4) promote private sector development of high quality security products and services.

1. Adopt the NII Security Tenets and the OECD Security Principles for use on the NII.

Sound security must be based on a common understanding of what is entailed. The NII Security Tenets previously proposed and the internationally-recognized OECD Security Principles [Appendix A] form a solid foundation for developing security products, services, and practices on the NII and internationally.

Furthermore, security is needed to protect privacy and intellectual property rights. Principles on privacy and on intellectual property rights have been released by both the U.S. Advisory Council on the NII and by the Information Infrastructure Task Force.

Proposed Action 1: *Promulgate the Tenets and Principles in the final version of this report by September, 1995.*

2. Stimulate dialogue and awareness of security risks, needs, and solutions.

The series of public meetings co-sponsored by the Security Issues Forum and members of the NII Advisory Council is the beginning of an on-going dialogue concerning NII security. This report is designed to further that dialogue.

As the NII interconnects U.S. participants into a global information infrastructure, it introduces new threats to U.S. systems and information. Some of these threats (e.g., sophisticated "crackers" in a foreign country) may be difficult for individual participants to fully perceive. In the course of its international relations, the Federal government may learn about the prevalence and magnitude of this type of threat. This information should be shared with participants in the NII.

During the public meetings, there was considerable discussion about assuring appropriate behavior on the part of participants in the NII. One part of that discussion pointed out that many of those who break into others' systems believe such behavior is acceptable. To begin countering this incorrect perception, it was suggested that the Federal government should promote inclusion of ethical computing in educational courses.

Proposed Action 1: *Develop data on threat and risk assessment for the NII and appropriately make it available to the public. Promote awareness of the existence of different threats to the NII with an understanding that there is no "one size fits all" solution, and that different threats must be treated differently. Ongoing.*

Proposed Action 2: *Stimulate dialogue and broad awareness of the national and economic security concerns related to the NII through public meetings and other outreach methods. Ongoing.*

Proposed Action 3: *Promote educational programs (along with the private sector and state, local, and tribal governments) to teach ethical behavior and awareness of security issues and risks on the NII. March 1996.*

Proposed Action 4: *Address the issue of minors gaining access to*

adult materials on NII. September, 1995.

3. Make Federal security products and techniques available for use in the NII.

This report recognizes that strong, effective security is important to users of the NII in protecting their information. In the past, when private sector products were not available, the Federal government has developed security products for its own use that other NII users have found useful. The Data Encryption Standard (DES) (Federal Information Processing Standard Publication 46), originally developed for government use, has become a worldwide standard for protecting financial information on the world's banking system. Similarly, the Digital Signature Standard (Federal Information Processing Standard Publication 186), provides a strong, efficient, and economical means of assuring the integrity of electronic documents and the authenticity of the sender. The extent to which government-developed technologies will be adopted by the private sector is dependent on a variety of factors. The government does not intend to mandate security products for private sector use, but instead to depend on the marketplace to select those products that best meet the needs of the various NII participants.

Proposed Action 1: Compile a list of security technologies developed for or used by the Federal government, evaluate them for appropriate and applicable use in the private sector, and make them generally available to the public. Ongoing.

4. Promote private sector development of high quality security products and services.

NII users are demanding high quality security products and services. Flexible and responsive standards and accreditation processes can assist in the development of those products.

Some security products may provide confidentiality of information that is so strong that it can frustrate law enforcement's authorized ability to listen to communications where criminal activity is suspected. As Vice President Gore has written:

"The Administration has committed itself to cooperating with industry representatives and privacy advocates towards the goal of developing a key escrow encryption system that will provide strong encryption, be acceptable to computer users worldwide, and address national security needs as well. Such a system would be implementable in software, firmware, hardware, or any combination thereof, would not rely upon a classified algorithm, would be voluntary, and would be

exportable. . . .

We also recognize that a new key escrow encryption system must permit the use of private-sector key escrow agents as one option. It is also possible that as key escrow encryption technology spreads, companies may establish layered escrow services for their own products. Having a number of escrow agents would give individuals and businesses more choices and flexibility in meeting their needs for secure communications." (Letter to Representative Maria Cantwell and others, July 20, 1994)

In addition, the Federal government has for years regulated the export of products based on critical technologies for national security reasons. Although the U.S. has relaxed many of its export controls for advanced computing and communications technologies, certain encryption technologies remain restricted. Nevertheless, the U.S. has committed to allowing the overseas use of encryption for personal use by Americans.

Proposed Action 1: Promote the development of private certification processes through private, nationally and internationally recognized entities such as the American National Standards Institute, the International Standards Organization, nationally recognized testing laboratories, Underwriter's Laboratories, and other private sector communities of interest, such as the health, entertainment, and financial sectors. June, 1996.

Proposed Action 2: Continue to work with industry to develop alternative key escrow technologies, to make available standards and technology for public use, to develop methods for providing compatibility among different key escrow technologies, and to consider ways to promote use of such technologies overseas. December, 1995.

Proposed Action 3: Work with industry and the private sector to foster development of a public key infrastructure. December, 1995.

Proposed Action 4: Encourage the private sector to develop technology vulnerability and risk management guidance in accordance with the requirements for their communities. December, 1995.

Proposed Action 5: Review technology policy for the NII to ensure support for cooperative Federal-industry approaches in the development of security technology. January, 1996.

Proposed Action 6: Issue a proposed rule to establish a personal use exemption for overseas use of encryption. July, 1995.

B. In its role as protector of the public interest, the government will: (1) assure adequate emergency response capability on the NII; (2) adapt current oversight processes to meet the challenges of the NII; (3) review criminal law; and (4) promote international cooperation.

1. Assure adequate emergency response capability on the NII.

Today the Federal government sets priorities and procedures for service on the public switched network in the event of an emergency in order to meet critical communication needs and to assist in an orderly recovery. This role should be extended to establishment of priorities and procedures to support a robust emergency response capability comparable to that provided by CERT, the Computer Emergency Response Team. An extension of this role to assure that priority communications in the NII when emergencies occur will be necessary.

Proposed Action 1: Review emergency communications and network services requirements and priorities, to include the Telecommunications Service Priority program, to assure that appropriate priorities for the NII are established in times of emergency. September, 1995.

Proposed Action 2: Cooperate with private sector and State, local, and Tribal governments to ensure that vital government and civil infrastructure security needs are being addressed. January, 1995.

2. Adapt current oversight processes to meet the challenges of the NII.

The government does not regulate the NII as a whole, although it does regulate different pieces, including providers such as common carriers and users such as financial institutions. As discussed above, virtually every sector of the economy, from health care to aviation, is growing to depend on the NII. Security failures in the supporting information infrastructure could jeopardize the U.S. economic well-being, national security, and public safety. Thus the current oversight processes must be adapted to meet the challenges of the NII.

Proposed Action 1: Examine whether current banking regulations are adequate in the areas of electronic banking, electronic payment systems, and "digital cash," in order, for example, to protect consumers from counterfeiting and fraud. November, 1995.

Proposed Action 2: Ensure that all Federal agencies evaluate their current oversight mechanisms and practices in light of the growing need to address the growing dependence on the NII.

December, 1995.

3. Review Criminal Law.

A review of current law is timely, particularly in the areas of intellectual property rights and computer crime. The Federal government has such reviews underway and will propose its views for public discussion in mid-1995. For example, the Intellectual Property Rights Working Group has proposed that selling software designed to defeat copy protection of copyrighted materials be deemed contributory infringement under the Copyright Act. The Federal government will continue to work with private sector and State, local, and Tribal governments to ensure that proposed changes in criminal law are appropriate.

Proposed Action 1: Propose legislation to enable prosecution of computer-related crime. June, 1995.

4. Promote International Cooperation.

In recognition of the increasingly global nature of the information infrastructure, the U.S. has been active in putting computer and communications security issues on the table in international fora. At the G-7 Ministerial Conference on the Information Society in Brussels in February 1995, the U.S. proposed, and the G-7 partners agreed, to increase efforts to find creative, technological and policy solutions to increase "the reliability and security of national and international networks . . . by developing security principles that are commensurate with the risk and magnitude of harm." The OECD has been a leading international organization in the area of information and communications security.

Proposed Action 1: Stimulate consideration of security issues at the OECD and other international fora. Ongoing.

C. The government will promote research and development in critical and high-risk areas.

Although the private sector will continue to respond to market pressures and opportunities to create technical security products, services, and techniques, there may be a need for government to encourage private sector research and development in high risk or critical technologies. Some technologies developed by the government which are suitable for adaption for industry applications sector may become available through technology transfer programs. In other situations, government supports the private sector through funding pre-commercial, pre-competitive technology through various grant programs,

cooperative research and development agreements (CRADAs), and other technology development programs. For example, the Advanced Research Projects Agency (ARPA) and the NIST Advanced Technology Program are currently funding research into advanced technology that could be used to support an automated copy management system.

Proposed Action 1: Promote research and development through the High Performance Computing and Communications Program, ARPA, NIST, and others, of security technology that supports agencies' missions. Ongoing.

D. As a user, the government has a responsibility to protect the information in its possession and to act as a model user. Thus, it has the obligation to support all elements of a secure NII as it procures and manages its own portion of the NII. The Federal government will: (1) protect its own security requirements through good management processes; (2) improve its national security/emergency preparedness capabilities; (3) ensure that the products and services it uses meet its needs; and (4) develop a security infrastructure for its own use.

1. **Protect its own information through good management practices.**

The Computer Security Act of 1987 provides the framework within which Federal agencies will manage the security of the vast majority of their use of the NII. Through that mechanism, they will work to assure the confidentiality, integrity, and availability of their information as they use the NII. In March, the Office of Management and Budget (OMB) issued a draft revision to OMB Circular A-130, Appendix III, "Security of Federal Automated Information" to re-orient Federal implementation of the Act. The proposal will guide agencies in securing information as they increasingly rely on the open and interconnected NII. It stresses management controls such as individual accountability and awareness and training, rather than technical controls.

Similarly, the military will use and be dependent on the security and reliability of the NII. This may require using technologies especially designed for government use, such as advanced firewalls and encryption devices.

Proposed Action 1: Release final guidance to agencies to assure adequate security of Federal automated information through education, training, and awareness programs across agencies. September, 1995.

Proposed Action 2: Continue development of security technologies

to support unique government requirements. Ongoing.

Proposed Action 3: Develop and implement a program to ensure the security of Federal automated information consistent with guidance. January, 1996.

2. Improve its national security/emergency preparedness capabilities.

The National Communications System is a government entity that seeks to effect coordination among Federal government agencies and between the government and the telecommunications industry in order to support the government's emergency response mission. Through its efforts to promote the sharing of information between the private sector and government, the NCS promotes greater cooperation in securing networks for both the civil and private sectors.

Proposed Action 1: Review and validate national security and emergency preparedness (NS/EP) requirements for the nation's information infrastructure. December, 1995.

3. Ensure that the products and services it uses meet its needs.

The Federal government will adopt voluntary, consensus based standards wherever practicable. Where an appropriate standard developed in the private sector is not available, government will develop a standard for its own use. These standards will be available for other parties to use on voluntary basis. These standards are developed and promulgated by the National Institute of Standards and Technology (NIST) of the Department of Commerce.

The Federal government has traditionally accredited many of its standards through government laboratories. Increasingly, however, private sector evaluations are encouraged, as in "Security Requirements for Cryptographic Modules" (Federal Information Processing Standards Publication 140-1). The government also publicly issues lists of commercial products that it has accredited for its use.

Proposed Action 1: Rely, where possible, on security products which are based on industry standards. However, where commercial security services and standards are insufficient for government's needs in the NII, the government should develop security standards and use products built to those standards. Ongoing.

4. Develop a security infrastructure for its own use.

Under the auspices of the NII Security Issues Forum, the General Services Administration has established a Security Infrastructure Program Management Office. This office is coordinating the development of a public key infrastructure to meet the Federal government's needs for digital signature and confidentiality purposes. The U.S. Postal Service is pursuing complementary efforts.

Proposed Action 1: Develop a public key infrastructure for government use. Demonstrate interoperability with multiple agencies and with industry. June, 1996.

V. CONCLUSION

Users of the NII require reasonable confidence about the confidentiality, integrity, reliability, and availability of their communications. While the Federal government has a role in supporting a secure NII by facilitating private sector activity, ensuring public safety by protecting against abuses that result in harm to others, and supporting research and development in critical areas, much of the responsibility lies with the private sector. It is neither appropriate nor realistic to expect the Federal government to provide the security solution for the NII. Not only is the NII too complex for a one-size-fits-all solution, but without demand from users, the market in appropriate security tools and services will not succeed.

Ultimately, users must realize that no system is completely free of risk. Users of the NII must make informed choices about an acceptable level of risk for a particular transaction. While laws, policies, and technology can contribute to a secure NII, awareness of risk is the foundation upon which a secure NII will stand.

Excerpt from the
Guidelines for the Security of Information Systems
of the

Organisation for Economic cooperation and Development

26 November 1992

V. Principles

1. Accountability Principles

The responsibilities and accountability of owners, providers and users of information systems and other parties concerned with the security of information systems should be explicit.

2. Awareness Principles

In order to foster confidence in information systems, owners, providers and users of information systems and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures, practices and procedures for the security of information systems.

3. Ethics Principles

Information systems and the security of information system should be provided and used in such a manner that the rights and legitimate interests of others are respected.

4. Multidisciplinary Principle

Measures, practices and procedures for the security of information systems should take account of and address all relevant considerations and viewpoints, including technical, administrative, organisational, operational, commercial, educational and legal.

5. Proportionality Principle

Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm, as the requirements for security vary depending upon the particular information systems.

6. Integration Principle

Measures, practices and procedures for the security of information systems should be co-ordinated and integrated with each other and with other measures, practices and procedures of the organisation so as to create a coherent system of security.

7. Timeliness Principles

Public and private parties, at both national and international levels, should act in a timely co-ordinated manner to prevent and to respond to breaches of security of information systems.

8. Reassessment Principle

The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.

9. Democracy Principle

The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.

**Statement of
Raymond G. Kammer
Deputy Director, National Institute of Standards and Technology
Before the
Subcommittee on Domestic and International Monetary Policy
of the
Committee on Banking and Financial Services**

October 11, 1995

Introduction

Good morning. Thank you for inviting me to testify before the Subcommittee. I am Ray Kammer, Deputy Director of the Commerce Department's National Institute of Standards and Technology (NIST). Under the Computer Security Act of 1987 and the Paperwork Reduction Act of 1995, NIST is responsible for the development of standards for protecting unclassified government computer systems, except those commonly known as "Warner Amendment systems" (as defined in Title 10 U.S.C. 2315).

In response to the topics in which the Committee expressed an interest, I will focus on the following:

- 1) an overview of encryption and digital signature technologies,
- 2) risks and hazards of using encryption,
- 3) the government's activities to find key escrow encryption solutions that balance the requirements of users, law enforcement and national security; and
- 4) the importance of taking a system-wide approach to security.

I. Two Fundamental Cryptographic Technologies - Encryption and Digital Signatures

For a future electronic environment for financial transactions, there are two important security technologies. Encryption protects the confidentiality of information while digital signatures help ensure its integrity.

A. Encryption - Protection of Confidentiality

First, *encryption* is one of the most cost-effective methods to provide for the confidentiality of information. Encryption transforms intelligible data into an unintelligible form. This is accomplished by using a mathematical algorithm and a "key" (or keys) to manipulate the data in a complex manner. The resulting enciphered data can then be transmitted without fear of disclosure, provided, of course, that the implementation is secure and the mathematically based algorithm is sound.

The original data then can be obtained through a *decryption* process. Knowledge of the particular key utilized for a particular encryption of data (or, in the case of asymmetric cryptography, knowledge of the associated key of the key pair) allows decryption of the information. For this reason, such keys need to be protected commensurately with the value of the information they protect.

One of the most widely used encryption algorithms is the federal Data Encryption Standard (DES), published by NIST as Federal Information Processing Standard (FIPS) 46-2.

Why is encryption useful?

Encryption can be used in many applications for ensuring confidentiality. It can be used to protect phone calls, financial transactions, computer files, electronic mail, electronic medical records, tax records, corporate proprietary data, credit records, fax transmissions and many other types of electronic information. It will be used extensively in the protection of electronic information and services.

Encryption of these and other records protects the individual privacy of our citizens including, for example, their financial records and transactions with government agencies and financial institutions. Private sector organizations also benefit from encryption by securing, for example, their product development and marketing plans. Encrypted data is, of course, useless to those without the decryption key. The government uses cryptography for the protection of its information -- from that involving highly classified defense and foreign relations activities to unclassified records, such as those protected under the Privacy Act.

B. Digital Signatures - Protection of Integrity

What is a digital signature?

A digital signature is created by electronically by applying the originator's private cryptographic key to the data. The resulting digital signature (a long numeric value) can be stored or transmitted along with the data. I should point out that I am speaking here of a signature that is a long mathematically generated number, not an electronic digitization of a handwritten signature.

The signature can be verified by any party using the public key of the signer (which may be available, for example, through an on-line directory for this purpose). If the signature verifies properly, then the verifier has confidence that the data was not modified after being signed and that the owner of the public key was the signer.

NIST has published standards for a digital signature and a secure hash for use by the federal government in FIPS 186, *Digital Signature Standard* and FIPS 180, *Secure Hash Standard*.

Why are digital signatures useful?

It is desirable to have an automated means of detecting unauthorized changes -- whether intentional or accidental. In computer applications, it is not always possible for humans to scan information to determine if data has been erased, added, or modified. While some modifications may be easy to discern, others may be less obvious. For example, "do" may be changed to "do not," or \$1,000 may be changed to \$10,000. Clearly, modifications of electronic financial data can have serious repercussions. Digital signatures provide a simple, cost-effective method to detect such changes to electronic data.

Digital signatures also provide a means to verify the origin of data. When a signature is successfully verified, the receiver (or any other party) has confidence that the message was signed by the owner of the public key and that the message has not been altered since it was signed. Digital signatures do not scramble data, and therefore do not render them unintelligible. While digital signatures and encryption are often used together, they serve very different functions.

II. Risks and Hazards of Using Encryption

Counterbalanced against its benefits, encryption also can present many substantial risks -- to *both* users and the government.

First and foremost, encryption can frustrate legally authorized criminal investigations by the federal, state, and local law enforcement agencies. For example, law enforcement personnel may, with proper legal authorization, record a phone conversation in the investigation of suspected criminal activity or seize stored data pursuant to a court ordered search warrant. If these communications or data seized are encrypted, law enforcement could be precluded from obtaining evidence crucial to the successful prosecution of activities that jeopardize the public safety. As their representatives can better explain, lawful electronic surveillance has proven to be one of law enforcement's most effective investigative techniques available to investigate serious criminal activities including organized crime, drug trafficking, and violent crimes. The ability to lawfully obtain the encryption keys necessary to decrypt these illicit conversations would help preserve this essential law enforcement tool.

Second, encryption may also prove a potential hazard to users, such as private sector firms, particularly as we move into the Information Age. Private firms too are concerned about the

misuses of cryptography by their employees. For example, a rogue employee may encrypt files and offer the "key" for ransom. This is often referred to as the "data hostage" issue. Keys can also be lost or forgotten resulting in the unavailability of data. To protect against such threats, some corporations have expressed interest in a corporate key escrowing capability to minimize harm to their organizations from internal misuse of cryptography. Additionally, users of encryption may gain a false sense of security by using poorly designed or implemented encryption. As security experts point out, such a false sense of security can be worse than if no security measures were taken at all.

Before moving on, you will note that I have not mentioned the risks of digital signatures. In general, since digital signatures do not provide for the confidentiality of data, they do not prevent law enforcement from accessing such data, and thus the risk to law enforcement and national security are minimized. With respect to digital signatures, users should recognize two important points. First, although digital signatures can effectively detect unauthorized modification of signed data, they cannot directly protect such modifications from occurring. Second, a digital signature only proves the identity of a signer if that signer has properly protected his or her key. If an individual's key has been disclosed to others, either intentionally or negligently, then others can sign documents with that individual's "signature."

III. Key Escrow: One Approach to Balancing Societal and User Interests

Because of the risks of strong encryption, the federal government is proposing to adopt key escrow cryptography for its own use. This technology allows the use of strong encryption, but also allows the government when legally authorized to obtain decryption keys held by escrow agents. On August 17, 1995, the Administration announced its intent to develop a federal standard for key escrow that would be implementable in software. This will allow agencies to choose between hardware and software-based approaches to accomplish key escrowing. NIST sponsored an exploratory workshop on September 15, 1995 to discuss various approaches to developing such a standard. We have just begun the task of putting together a proposed approach to this standard. You should be aware that we envision the escrowing of keys that allow the "unlocking" of encrypted information; in general, we do *not* foresee the escrowing of keys that are used only for signature purposes.

In 1994, NIST published the *Escrowed Encryption Standard* as FIPS 185 which is a hardware-based approach. Currently this standard is applicable to telephone communications; however, we intend to propose a modification to allow federal agencies to also use compliant products in data application environments.

As I stated earlier, private sector organizations also have developed an interest in key escrowing, but from a slightly different perspective. Many organizations, including government agencies that use encryption, have realized the need to protect themselves against inadvertent or deliberate actions that may result in the unavailability of encryption keys. Industry is responding to this need by developing commercial key recovery products.

IV. Achieving Security of Information and Systems

Both encryption and digital signature can provide important protections. However, their limitations must be recognized. These technologies also must be used correctly so that their benefits can be obtained. Let me briefly elaborate.

Cryptography is not a cure-all.

I will not belabor this point but it is important: use of cryptography is not a security cure-all. Encryption and digital signatures have many important applications for the confidentiality and integrity of data. But they cannot solve all security problems -- after all, systems are used and managed by people, who are the greatest security risk.

Cryptography must be based on sound principles and correctly implemented.

Cryptographic security measures must be correctly and securely implemented. It is perhaps intuitively obvious that algorithms must be mathematically strong against attack. Moreover, they must be correctly implemented and the cryptographic keys appropriately protected. Testing of cryptographic products can help provide assurance of correct and secure implementation.

FIPS 140-1, *Security of Cryptographic Modules*, and its associated validation program provide specifications for secure cryptographic modules and assurance of correct implementation.

Cryptographic controls do not function in a vacuum.

Perhaps less obvious and more often forgotten is that complementary security controls need to be in place to support cryptographic security measures; they cannot be fully effective without the presence of supporting managerial, administrative, physical, and personnel controls. For example, appropriate physical access control to an encryption device is necessary in order to prevent unauthorized changing of cryptographic keys. Moreover, the security of a system must be evaluated on more than just the cryptographic security measures used. As I mentioned earlier, technology is not independent of its human users and managers. These individuals pose risks to the system as well as the means to actually secure information and systems.

Management must make appropriate risk-based decisions.

In electing to take advantage of encryption and digital signatures, cognizant management officials need to understand their threat environment, the benefits, limitations and risks of using cryptography, and the costs associated with using, or not using, such security measures. For example, managers need to think carefully about the benefits of protecting their information versus the risks of losing data if cryptographic keys suddenly become unavailable.

One of the most important decisions to be made in choosing cryptographic security measures is

selecting between hardware and software implementations. Hardware implementations, whether of encryption or digital signatures, are much more resistant to unauthorized modification. If someone has access to a software product (or the system upon which it is run), one can alter the functioning of the product or obtain the encryption key. People inside organizations have direct access and individuals outside the organization often have potential remote access to systems; this offers the opportunity to change software, either intentionally or unwittingly. Without extensive (and expensive) protective measures, one cannot be assured that a software implementation of an encryption algorithm will not be altered in such a way as to undermine the strength of the encryption or digital signature. Such changes are much more difficult to do with hardware-based cryptography. Therefore, the assurance that users can have of their continued security is greatly enhanced through the use of hardware-based cryptographic technologies.

Within the federal government unclassified sector, I believe that high value information should be protected by hardware-based products. Agencies may accept the risk of lower-cost software cryptography for lower value information, but they need to be aware of the attendant risks and uncertainty of whether or not the product's security remains assured. Agencies, as the direct custodians of their information, are in the best position to make these risk-based decisions, and determine which of their data are more important and require hardware-based cryptographic security measures.

Finally, let me briefly explain the federal government's approach to use of cryptography, which I like to characterize into three categories. First are classified applications, for which the Department of Defense's National Security Agency's classified cryptographic technologies apply. Secondly are those unclassified applications of "high value," as determined by the owner of the data. This may include data whose unauthorized release could seriously impact the ability of the agency to accomplish its mission. It is for such uses that NIST recommends high-assurance cryptographic products, generally hardware-based implementations. For other unclassified applications when cryptography is called for, software-based implementations may be appropriate, provided that the attendant risks are understood.

Summary

Encryption and digital signature technology will play an increasingly important role in the protection of electronic financial systems, transactions, and records. Attendant with the potential benefits of encryption are risks to law enforcement and national security. These can be dealt with through the use of key escrow systems. Cryptography does not provide a single cure-all to protect systems and information; complementary controls are also necessary.

Thank you, Mr. Chairman. I would be pleased to answer your questions.

MR. RAYMOND G. KAMMER

Deputy Director

National Institute of Standards and Technology

Raymond G. Kammer is the Deputy Director of the National Institute of Standards and Technology. He has served in this capacity from 1980 to 1991 and from 1993 to the present. Mr. Kammer is responsible for the day-to-day operation of the Institute and for long-range planning and policy development. The primary mission of NIST is to promote U.S. economic growth by working with industry to develop and apply technology, measurements, and standards. This mission is accomplished through four major programs:

- a competitive Advanced Technology Program that provides cost-shared awards to industry for development of high-risk technologies with significant commercial potential;
- a grassroots Manufacturing Extension Partnership designed to help small and medium-sized companies adopt new technologies;
- laboratory research and services focused on "infrastructural technologies," such as measurements, standards, evaluated data and test methods; and
- the Malcolm Baldrige National Quality Award and an associated quality outreach program.

The NIST budget is \$600 million. The staff of approximately 3,000, of whom more than 1,600 are scientists and engineers, are located at campuses in Gaithersburg, Maryland and Boulder, Colorado.

From 1991 to 1993, Mr. Kammer was Deputy Under Secretary of Commerce for Oceans and Atmosphere in NOAA. In that position, he served as NOAA's Chief Operating Officer and was responsible for overseeing the technical projects of this \$2 billion agency which has a staff of over 14,000. NOAA has five major programs - the National Weather Service; the National Marine Fisheries Service; the National Environmental Satellite, Data, and Information Service; the National Ocean Service; and the Office of Oceanic and Atmospheric Research.

Mr. Kammer began his career with the Department of Commerce in 1969 as a program analyst. Prior to his appointment as Deputy Director of NIST, Mr. Kammer held a number of positions at NIST and in the Department of Commerce involving budgetary and program analysis, planning and personnel management. During his tenure as Deputy Director, he also held positions as Acting Director of NIST, Acting Director of the National Measurement Laboratory at NIST, and Acting Director of the Advanced Technology Program at NIST.

Mr. Kammer has chaired several important evaluation committees for the Department of Commerce, including reviews of satellite systems for weather monitoring and the U.S. LANDSAT program, and of the next generation of weather radars used by the U.S.

government. He also served on the Board of Directors of the American Society for Testing and Materials, a major international society for the development of voluntary standards for materials, products, systems, and services.

His awards include both the Gold and Silver Medals of the Department of Commerce, the William A. Jump Award for Exceptional Achievement in Public Administration, the Federal Government Meritorious Executive Award, and the Roger W. Jones Award for Executive Leadership.

Mr. Kammer received his Bachelor of Arts degree from the University of Maryland in 1969.

STATEMENT
TO THE
SUBCOMMITTEE ON DOMESTIC AND INTERNATIONAL
MONETARY POLICY
OF THE
COMMITTEE ON BANKING AND FINANCIAL SERVICES,
U.S. HOUSE OF REPRESENTATIVES

HEARING
ON THE FUTURE OF ELECTRONIC FORMS OF MONEY
AND ELECTRONIC PAYMENT SYSTEMS

BY
WILLIAM P. CROWELL
DEPUTY DIRECTOR,
NATIONAL SECURITY AGENCY

11 OCTOBER 1995

Introduction

Mr. Chairman and distinguished members of the Subcommittee, I appreciate the opportunity to appear before you this morning. I am Bill Crowell, Deputy Director of the National Security Agency. I am here today to discuss the efforts of the Department of Defense to provide security for its information systems.

Growing dependence on information infrastructures

We have entered the information age. Just as control of industrial technology was key to military and economic power during the past two centuries, control of information technology will be vital in the decades ahead. Nations are daily becoming more dependent on networked information systems to conduct essential business, including military operations, civil government, and the operation of national and international economies.

Vulnerability of networked data and systems

The increased efficiency, productivity, and cost savings of networking come at the price of increased vulnerability of data and systems to attack. Information in unprotected or poorly protected networks can be accessed, changed, or destroyed. Unprotected systems can be controlled, damaged, or shut down. Through global interconnectivity, targeted systems can be accessed and attacked from almost anywhere in the world.

INFOSEC: Data integrity Authentication of users Non-repudiation assurance Confidentiality of data Availability of service

The vulnerabilities associated with networking have fundamentally changed the nature of our information systems security mission. In the pre-network era of point-to-point circuits, we focused primarily on protecting the confidentiality of information. In the networked environment, information systems security, or INFOSEC, includes not only confidentiality but protection of systems from viruses and other attacks intended to deny service, protection of data from alteration or destruction, and assurance that data exchanges are originated and received by valid participants.

Our Information Infrastructure Is at Risk

Our vulnerability is unprecedented

At their current stage of development, the Defense and National Information Infrastructures offer minimal defense against unauthorized access and use. As a result, DoD and the nation are vulnerable as never before to theft of information and to large-scale disruption through data corruption or system shut-downs.

**How do we know
we are vulnerable?**

How do we know that our infrastructure is vulnerable to these types of attacks? We know both through test attacks conducted against our own Defense networks, and through clear and abundant evidence that our vulnerabilities are being exploited today.

**We know through
test attacks against
our systems**

Tests conducted last year by the Defense Information Systems Agency (DISA) demonstrated the vulnerability of DoD unclassified logistics, support, and medical networks. Using widely available techniques, DISA experts attacked nearly 10,000 DoD computers, successfully gaining access to 88 percent of them. Only four percent of the successful penetrations were detected by the organizations under attack. Of those organizations detecting attacks, only five percent reacted. Overall, during these tests only one in roughly a thousand successful attacks drew an active defensive response. Based on these results and the current level of reported security incidents, the number of penetrations of DoD systems during 1994, including those undetected or unreported, has been estimated at 300,000.

**We know through
increasing real-world
attacks against DoD
systems**

There is ample evidence that the vulnerabilities noted in DISA's testing have been found and exploited by real-world attackers. During 1994, more than 250 unclassified DoD computer systems were known to have been penetrated by outsiders. Functions supported by the compromised systems included weapons and supercomputer research, logistics, finance, procurement, personnel management, payroll, and military health systems. The attackers stole data, destroyed data, modified software, installed unwanted files, and crashed systems. The incidence of such attacks is escalating and the number is projected to double this year.

Let me give you some examples that demonstrate the scope of this problem. Administrators of one Pentagon system suspected they had a minor security problem with intrusion attempts over the Internet. When user access was monitored, 4,300 unapproved intrusion attempts were detected during the first three months of the monitoring effort. Administrators of another system stumbled onto what they thought was a high school hacker. When the system was monitored for access, it was found that hackers from 14 different countries were attacking the system.

**Other federal users and
the private sector are
equally vulnerable**

The networked systems serving the rest of the Federal government and the private sector are equally vulnerable. Known targets have included financial systems, payroll systems, personnel records, industrial research and development information, tax files, and credit card files. One recent press report estimated U.S. losses from computer crimes via the Internet within the past year

alone at \$5 billion.

**Vulnerability of
critical systems**

The demonstrated vulnerabilities of our information technology entail a potential vulnerability to economic disruption on a very large scale. The phone system, the banking, credit, and Federal Reserve systems, the stock exchanges, the power distribution system, the air traffic control system, public safety, and law enforcement all depend heavily on networked information systems. These functions are all potentially vulnerable to network-based attack and disruption.

**INFOSEC:
Key enabling technology
for the information age**

The vulnerability of the U.S. information infrastructure makes information systems security a key enabling technology for the information age. Within the Department of Defense, a broad partnership of Defense agencies is working to reduce the vulnerability of the Defense Information Infrastructure.

**Reducing Defense Information Infrastructure
Vulnerability**

**DoD INFOSEC Strategy:
roles of NSA, DISA,
and ARPA**

The DoD has developed an integrated strategy to protect its information and information systems. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence has taken the lead in supporting NSA, DISA, Advanced Research Projects Agency (ARPA), and the military departments in carrying out these efforts. Within this strategy, NSA provides DISA with the tools, techniques, products, services, and security management structures needed to protect the Defense Information Infrastructure (DII). DISA plans, engineers, implements, operates, and manages the system, providing the DoD's first line of defense for detecting intrusions or attacks. By analogy, NSA supports DISA in much the same way that Bell Labs supported the AT&T system's operating companies. In the area of long-range INFOSEC research, NSA and ARPA are now coordinating their programs, in partnership with DISA, to maximize support for DII security requirements.

**Key strategic goal:
interoperability**

These agencies are working together to incorporate full interoperability into the DII security architecture. Given the limited resources available for INFOSEC, it is critical that we get interoperability right the first time and avoid the expense of having to backfit secure connectivity across systems that have evolved in incompatible ways. The expense of such a corrective retrofit effort would be staggering.

**Networked systems
need multilevel
security**

In working to provide INFOSEC for the emerging DII, DoD faces a key challenge in providing for multilevel security. In the past, classified information moved over dedicated circuits and was stored and processed by stand-alone computers. To fully utilize the capabilities of networked systems, users need the ability to manage and distribute data of different security sensitivities over common networks. Multilevel security is essential to secure information system integration.

**MISSI:
the Multilevel
Information Systems
Security Initiative**

The cornerstone of DoD's effort to provide multilevel security for the DII is our Multilevel Information Systems Security Initiative (MISSI). MISSI includes a number of ongoing and planned efforts to make available INFOSEC products and services for workstations, local area networks, and wide area networks. These will serve as common building blocks that can be combined to provide tailorable security capabilities according to individual users' needs. MISSI will also provide products and services for common network security management. Working in integrated architectures, MISSI products will protect data from unauthorized disclosure and modification, identify and authenticate system users, control access to data and systems, and verify the originators of incoming messages. MISSI is intended to reduce the duplicative hardware and personnel overhead costs associated with current policies governing the use of information systems to process classified information.

**MISSI:
An architecture based
on commercial standards**

In essence, MISSI is a framework. With the MISSI approach to interconnected networks, we've distilled our military security needs into an architecture, supported by industry standards and commercial products. In the future, the MISSI architecture will allow us to satisfy our security needs with commercial products, evaluated as having achieved a specified level of assurance, compliant with the architecture, and configured to deliver security services tailored to the users' requirements.

**The FORTEZZA
cryptographic card**

While our longer term strategy is to have industry become the primary developer of MISSI compliant products, we have moved to jumpstart MISSI with several government-designed products and their supporting infrastructure. The first high-volume product within the MISSI architecture is the FORTEZZA cryptographic card. The FORTEZZA card is a hardware-based encryption product. It is the size of a thick credit card and plugs into its host platform, such as a desktop or laptop computer or a digital personal communications device, using the international commercial standard PCMCIA interface. FORTEZZA cards will be

produced by multiple vendors, but will be functionally identical. The first generation of FORTEZZA cards, intended for use with unclassified but sensitive information, went into production over the past year. The next phase will be to provide security for applications with classification levels up to secret.

FORTEZZA capabilities

FORTEZZA functions include encryption and decryption, digital signature, and a hashing algorithm to ensure integrity, providing its users with authentication, confidentiality, data integrity, and proof of delivery and origin for a variety of applications. A user can access FORTEZZA security services with a personal identification number used in conjunction with a personalized FORTEZZA card. FORTEZZA secured applications include electronic mail, electronic commerce and electronic data interchange, file transfer, file storage, remote database access, World Wide Web browsers, and remote identification and authentication.

Partnership with industry

We are working with leading information technology corporations to ensure that their commercial applications and operating systems will operate with FORTEZZA. Industry leaders working with us to provide FORTEZZA-enabled products include Microsoft, Lotus, Novell, Banyon, Netscape, Simplex, Oracle, IBM/Triteal, Hughes, and Qualcomm.

Need for supporting security infrastructure

To provide interoperable security services across the DoD, FORTEZZA will require extensive infrastructure support. Establishing a security infrastructure on a DoD-wide scale is one of the key challenges in implementing the MISSI approach. The extent of the security structure supporting the FORTEZZA card can be envisioned by analogy to that supporting credit cards. Credit card companies must have a structure to keep track of which individuals are authorized to have credit and to what level. The structure must allow this information to be accessed by the stores wanting to make sales. It must allow for identification of the individual, and keep the information accurate and safe from unauthorized access. It must do this in a user-transparent way.

The infrastructure challenge

Similarly, network security management products and services will provide support for FORTEZZA. This support includes a network of certification authority workstations, repository services for centrally accessible security information such as digital signature certificates, and access control. Building an infrastructure capable of supporting the security requirements of the Department of Defense requires a unifying vision and long-term commitment.

**Interoperability
with software-based
solutions**

FORTEZZA is intended to support classified applications up to the secret level and high value unclassified applications. As a hardware encryption product, it offers a higher level of assurance than software encryption products, but at a higher cost than software. We recognize that many of DoD's commercial partners may prefer to use software encryption on the basis of cost, and intend to ensure that the hardware and software tiers will be able to communicate. It is planned that FORTEZZA will interoperate with software-based solutions under some circumstances.

**Encryption alone
cannot ensure security**

We believe that FORTEZZA will provide a very secure approach to encryption services. We also recognize that high-quality security technologies alone are not sufficient to secure the DII. Also needed are INFOSEC customers with the knowledge to implement and use the technology effectively and workable doctrine and procedures. Security solutions must encompass managerial, administrative, physical, and personnel controls. Encryption without adequate supporting procedures is like a bank vault door on a cardboard box.

**Risk is inherent
in networking**

With the best of precautions, in a networked environment some risk will remain. With information technology advancing dynamically, no solution can be considered perfect. To realize the efficiencies of networking, one must accept risk and manage it. Risk management will be a critical skill in the information age.

**Defense and National
Infrastructures have
parallel security needs**

The broad security needs of the entire National Information Infrastructure (NII) closely parallel those of the DII. Like the DII, the NII must have secure and reliable networks that support interoperability among its users, including government agencies, businesses, and the general public. We in DoD hope that the experience of developing FORTEZZA as a single standard for DoD computer-based encryption will provide useful lessons as the nation moves to provide security for the NII. We are working to migrate our technology and experience into the civil government and private sectors through our partners at NIST. I wish to emphasize that we do not have the only solution. This task is huge and will require contributions from many sources. Collaboration among many partners will be essential.

**Defense experience
with FORTEZZA may
prove useful**

Mr. Chairman, this concludes my prepared remarks. I would be pleased to answer any questions you may have. In addition, if time permits, I would like to conclude my testimony today with a brief demonstration of DoD's FORTEZZA solution.

**Statement of Philip N. Diehl
Director, United States Mint
before the
House Subcommittee on
Domestic and International Monetary Policy
"The Future of Money"
October 11, 1995**

Mr. Chairman, and Members of the Subcommittee, I would like to thank you for inviting me to testify on the "Future of Money". As you know, Mr. Chairman, the Mint has taken a strong and active interest in this matter and has begun work to address certain policy issues related to it. I welcome your interest in this matter and the leadership you have shown in calling this series of hearings.

As the Subcommittee may be aware, the Mint is participating in the Treasury Department's Electronic Money Task Force, headed by Comptroller of the Currency Eugene A. Ludwig. The Task Force, which convened for the first time last month, will coordinate the efforts of the various bureaus and agencies of the Department of the Treasury, providing a source of common information to be shared among the bureaus while allowing each to pursue initiatives specific to its mission.

The Mint's main interest in the evolution of payments systems is related to stored-value cards as a potential substitute for coins and currency. As sole provider of the Nation's coinage, the Mint has an important role in our monetary system. As the use of stored-value cards evolves, many consumers might be expected to replace coinage and currency transactions with "e-cash" transactions, thus creating a de facto new form of currency. We believe that such a scenario must be studied comprehensively so the Federal government will be prepared to address the policy and legal questions that a new form of currency would present.

Mr. Chairman, as I have testified to this Subcommittee in the recent past, technological advances affect every part of our lives, including our currency. Coins are a declining "second wave" technology of commerce; what we are wrestling with here today are the implications of these emerging electronic "third wave" substitutes for coinage. I think we can be informed by an interesting historical analogy related to the evolution of paper currency during the first half of the 19th century. In the decades preceding the Civil War, to meet the demands of commerce for which U.S. coinage was inadequate, a multitude of local and state banks issued their own bank notes. These traded at face value in the immediate vicinity of the issuing banks but at a substantial discount, or not at all, elsewhere.

As interstate commerce expanded and private banks failed or merged, the limits of this private system of currency became obvious. By 1860, the currency market was in chaos. The financial requirements of the war led President Lincoln to preempt the local banks and issue our first national currency in order to facilitate interstate commerce.

Clearly, we do not face the urgency of a national crisis today. However, as you and I are aware, Mr. Chairman, private parties in a variety of industries are proceeding rapidly to develop their own versions of "e-cash" systems. It is appropriate to ask the question whether at some point in the future the requirements of market efficiency could accelerate the Federal government's role in producing a stored-value card that would augment the use of coinage in commercial transactions. The issuance of a "legal tender" stored-value card would also allow the Treasury to retain seigniorage profits that would otherwise be reduced by a decline in the demand for coinage, avoiding the need for additional tax revenue or additional borrowing.

But, Mr. Chairman, questions related to such a significant change in our Nation's currency

are not to be taken lightly. They must be carefully studied, and if governmental involvement is deemed necessary and appropriate, we must define a role that accommodates the emerging "e-cash" systems of the private sector.

Mr. Chairman, I have attached for the Subcommittee's review a copy of the Mint's Reinventing Government II (REGO II) proposal offered as part of Vice President Gore's National Performance Review. This proposal was one of seven that the Department of the Treasury forwarded to the Vice President.

In a nutshell, the Mint has proposed that the Treasury Department take the lead in identifying and addressing policy issues related to stored-value and smart cards as substitutes for currency, with participation by other Treasury bureaus, the Federal Reserve, other Federal governmental agencies and departments, and the private sector. As electronic forms of payment become more commonplace, reducing the demand for coinage and currency, and in effect becoming a new form of currency, the Federal government must be prepared to address the policy concerns that will arise.

Already, major financial services providers are taking to market stored-value and smart cards. In Great Britain, National Westminster Bank has created the Mondex card, a smart card that acts as a substitute for cash. The card allows for electronic transfers of value from one person directly to another person or business using an off-line system, without the intermediation of a financial institution. Earlier this year, Mondex launched its first trial in England, and franchises have been granted or are pending in several countries in the Far East and in Canada. Mondex is even in use in the United States, in a trial partnership program between National Westminster and Wells Fargo Bank in San Francisco.

This one example is evidence of the need for the Federal government to quickly and comprehensively evaluate the evolution of payments systems and substitutes for currency and be prepared to act accordingly, if deemed necessary and appropriate. That was the impetus behind the Mint's REGO II proposal.

As you know, Mr. Chairman, the seigniorage from circulating coinage is a major source of revenue for the Treasury, and the sale of U.S. commemorative coins is also a revenue raiser for the government. As electronic forms of payments become more widespread, the demand for and thus supply of coinage will decrease, and so will the revenue raised from seigniorage. However, the idea of a Treasury-issued, "universal" stored-value card presents the potential for recouping the lost seigniorage revenue from a lower demand for coinage, especially considering the high dollar value that could be stored on such a card. While this idea may seem arcane, and is admittedly complicated, it is worth exploring and will be covered in detail in the Mint's REGO II study.

Mr. Chairman, the evolution in electronic payments systems presents interesting new opportunities for the Federal government to recognize new revenue streams. I look forward to the Mint's continued involvement in this issue, and I look forward to further working with you as the Federal government readies itself to address the many issues raised by these swift changes.

NATIONAL PERFORMANCE REVIEW - PHASE II
DEPARTMENT OF THE TREASURY - FINAL PROPOSALS

Commission Study of Currency Smart Card

Proposal

This initiative proposes conducting a study to determine the feasibility of an electronic smart card. The card would actually function in lieu of coins or currency, because monetary value would be transferred directly to the card (as opposed to the card simply giving a payee access to a consumer account from which payment is to be made, as is the case with debit and ATM cards).

The three aspects of Treasury's providing a smart card are as market maker (setting regulations, standardization, security); provider of government services, such as electronic benefits transfer; provider that competes with other private sector providers of smart cards.

The initial study group would be composed of representatives from federal departments, the Federal Reserve Board, and private industry. There would be no substantial additional costs to the government to conduct the study, beyond some consulting fees; staff costs will be drawn from existing Departmental resources

Projected Cost/Benefit Analysis
(\$ in millions)

	Estimated Change to FY 1996	Estimated Change to FY 1997	Estimated Change to FY 2000	Five-Year Cumulative (FY 1996-2000)
Government-wide Costs	\$0.3			\$0.3
Potential Savings from Implementation			\$10.3	\$10.3

Background

The current system of circulating coinage and currency in the United States was designed to facilitate day-to-day commercial transactions between consumers and retail providers of goods and services. When first implemented, this system provided a convenient means of exchange for household goods and day-to-day items.

Inflation has led to the devaluation of money and, as a result, consumers now must carry larger denomination amounts on-hand. (For example, inflation has decreased

Department of the Treasury

dramatically the value of the penny; consumers now often view the penny as a disposable coin). Consumers are reluctant to carry large volumes of cash, and the demand to carry out "cash-less" transactions has been met by an increase in retail acceptance of credit cards and ATM-type bank cards. Many functions that were carried out with the use of coins and low denomination currency, such as telephone services and day-to-day retail transactions, now can be performed with the use of a debit card. The wide use of such means of payment illustrates the rising comfort level among consumers with electronic transactions.

Further technological advances have allowed the discussion of commerce in the future to include proposals of an entire "cash-less" society. "Smart cards" contain an integrated circuit and are more similar to a hand-held computer than to a debit or credit card. These cards will be the next development in the revolution of payment methods for retail goods and services. Because of its mission, Treasury has significant interests in this new technology.

Analysis

The NPR's Decision Tree for Analyzing Agency Programs provides the basis for the discussion outlined below:

Step 1--Is this program or function critical to the agency's mission based on customer input?

Yes. Consumers are reluctant to carry large amounts of cash because of security issues; they are relying increasingly on non-cash methods of payment. An electronic currency smart card could be issued, functioning much like credit, debit, and ATM cards issued by commercial banking, consumer credit, and information services companies. Currency smart cards could be used at retail outlets as means of payment for goods and services in the same way that credit, debit, and ATM cards are currently used.

These smart cards would allow consumers to add to or subtract monetary value. Such transactions would be performed by transferring funds from existing accounts, either in person at commercial banks or other institutions where money is deposited, or electronically, through ATM machines, over the phone, through personal computers, or by other methods that future technological advances in information services will allow.

Step 2--Can it be done as well or better at the state or local level?

No. The U.S. Constitution empowers Congress to coin money. The Federal Reserve determines the paper currency requirement as an incremental part of the total money

Currency Smart Card

2

Department of the Treasury

supply. Monetary policy is the exclusive domain of the Federal Reserve and is independent of the Executive Branch of the government by statute.

Step 3--Can it be privatized or terminated?

Yes. The use of electronic payment methods, such as debit cards, has increased substantially in the past few years. The federal government has already begun to utilize electronic benefit transfer methods, as evidenced by a pilot partnership program between the Financial Management Service (FMS) and private industry for the conveyance of federal benefits.

Step 4--Is there any way to cut cost or improve performance by introducing competition?

Yes. However, the government is in a unique position to drive this technology to commercial critical mass, establish universal standards for the entire industry, and promote its widespread implementation among state and local governments and transfer its technology to federal programs.

Description of Proposal

A study would be implemented to determine (1) the feasibility of a private/federal partnership to promote and develop a currency smart card; and (2) the effect this currency card would have on the money supply (circulating coin and paper currency) and monetary policy.

Coupled in a partnership with private industry, the federal government could lead the way toward an information-based economy and facilitate development of the most efficient, cost-effective, and convenient system of payment for commercial transactions, using all available resources and technological advances.

The study group would be composed of representatives from the federal departments, the Federal Reserve Board, and private industry. The commission would be a part-time entity, and would not require full-time participation of representatives. The commission would also invite participation from private industry representatives such as the American Banking Commission.

An outline of several critical issues that should be addressed by this commission are identified in the "Challenges" section below.

*Department of the Treasury***Implementation Options**

This proposal could be implemented in conjunction with the eliminating the penny from circulation and substituting in the dollar bill with the dollar coin.

Benefits

- Widespread acceptance, among consumers and businesses, of an electronic currency smart card would dramatically reduce the demand for circulating coinage and paper currency. This in turn would reduce the need for production of coinage and currency.
- For businesses, costs of physically handling and safekeeping coins and currency would decrease, and a more convenient method of payment could translate into higher sales. Also, an instantaneous transfer of funds would reduce costs associated with accepting checks as payment.

Challenges

- Monetary Policy: What impact will this proposal have on the money supply? What position will the Federal Reserve Board take on this proposal? How will this card effect overseas currency holdings? Can this card be considered legal tender? What impact would the announcement of this Treasury study have on international financial markets ?
- Consumer Acceptance: Will the general public accept a radical change in the way it does its day-to-day business, from a system of cash-based transactions to a system of electronic transactions? Will businesses embrace such a system, making use of a currency smart card the accepted means of payment?
- Equity: How would introduction of the smart card affect low-income citizens?
- Cost/Benefits: What will be the cost to the economy of implementing such a system? What will be the benefit to the economy implementing such a system? Will the initial costs incurred be offset by increased economic activity due to convenience and the decrease in costs of handling and safeguarding physical currency?
- Security: What would be the value to the public and the economy overall of the enhanced security of funds that a currency smart card would provide? Would use of the currency smart card increase the workload of Treasury enforcement

Department of the Treasury

agencies? Does fraud associated with electronic payment options increase the cost of the card?

- Benefits of Universal Debit Card Technology: In what other ways could such technology be used to make business and day-to-day transactions more efficient and convenient?
- Federal Government Leadership: Is it appropriate for the federal government to take the lead role? In what other areas and programs of the federal government could this technology be utilized? Will the currency smart card be attacked as a "Big Government/Big Brother" tactic?
- Environmental Considerations: Are there significant environmental benefits inherent in substituting a recycled plastic card for metal-based industrial process-intensive coinage?
- Cash Management: What are the cash management policy implications of using these cards? Can the government earn interest on the unexpended amounts on these cards? Can the government avoid borrowing?

Conclusion

While the prospect of a currency smart card may offer great benefits, a move toward a system of "cash-less" transactions is not one to be taken lightly. The Treasury Department should commission a comprehensive study of issues surrounding the production and issuance of a currency smart card in order to make an effective argument for such a change to Congress and the American people.

Implementation

Goals

Conduct a comprehensive study to assess whether production and issuance of a currency smart card would facilitate a more efficient, cost-effective, and convenient means of carrying out day-to-day consumer transactions, increase revenues, and reduce costs to the federal government and to the Treasury.

*Department of the Treasury***Means**

The study would be carried out by a commission comprised of representatives from federal government departments and agencies whose jurisdictions would feel the greatest impact. These would include, but not be limited to, representatives from the Departments of Commerce, Transportation, Health and Human Services, and Treasury, and the Federal Reserve Board.

Design

In order to accomplish this goal, OMB and Departmental approval to establish this commission, and a detailed marketing plan to educate Congress, the press, and the public are required.

Process

The decision process will require three steps:

- Step One: commission a comprehensive study on the feasibility of producing and issuing an electronic currency smart card;
- Step Two: examine the impact on the money supply; and,
- Step Three: if the project is practical, implement the use of a currency smart card.

Possible Performance Measures

- Market growth in private sector activity
- Demand changes in small denomination currency and circulating coinage

Data Assumptions

Government Estimated Costs

The estimated cost of \$0.3 million was based on costs of similar study performed within the past year (on "Currency Redesign"). This proposal assumes that there would be no substantial increased cost to the government since the study group would be composed of representatives from federal departments with volunteer participants from private industry.

Potential Savings from Implementation

The savings included in this paper could occur whether the card was a product of the private sector or a government-issued card.

These savings assumes that there will be a 2% *reduction* in demand in coinage and currency with a corresponding manufacturer cost decrease totaling \$13.0 million beginning in FY 2000.

Estimated savings are based on a reduction in future projected demand. The demand for coinage and currency, especially in recent years, has increased, primarily due to the expanding international economy's use of U.S. currency. Due to this rapid expansion, no statistical evidence is available that correlates to the expansion of the electronic payment methods to a reduction in demand.

Summary Cost Savings (\$ in millions)

	Discretionary Appropriation	Mandatory Appropriation
U.S. Mint	\$0.8	\$3.2
BEP		\$7.1

Other Considerations

Numismatic Market: If the study recommends the manufacture of a U.S. Treasury currency card, there is potential to develop a large numismatic market for these cards as collectibles. Information service companies who issue debit cards to customers have already experienced a demand for collectible versions of their cards, and collectible debt cards are the fastest-growing segment at a wide variety of shows. Increased revenues from this market are estimated at \$50 million.

Seigniorage: Currently, seigniorage is created through the government's sovereign power to create value from base metal in the creation of coins. Unlike coins, the Federal Reserve Board reimburses the Bureau of Engraving and Printing for its costs in producing currency. The concept of seigniorage accounting does not apply to currency at this time.

The study needs to explore the possible conceptual difference between the use of seigniorage today and the impediments to applying seigniorage accounting to the currency smart card. The adjustments in value proposed for the currency smart card are a departure from the current definitional treatment of seigniorage on the government's accounts.



Comptroller of the Currency
Administrator of National Banks

Washington, DC 20219

November 13, 1995

The Honorable Jack Metcalf
U. S. House of Representatives
Washington, D.C. 20515

Dear Congressman Metcalf:

I appreciate having had the opportunity to testify on electronic money before the Subcommittee on Domestic and International Monetary Policy on October 11, 1995. During the question and answer period, you asked me a question regarding why there are so few United States currency notes in circulation.

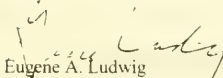
Although the Office of the Comptroller of the Currency historically played a role in currency matters, it currently has no involvement in this area. Today, the Office of the Comptroller of the Currency is primarily responsible for regulating and supervising national banks. As you know, technical amendments in the Riegle Community Development and Regulatory Improvement Act of 1994 (CDRI Act), Pub. L. No. 103-325, 108 Stat. 2160, ended what then remained of the Comptroller's limited role in currency matters by repealing obsolete statutes and transferring those functions that are still viable to the appropriate bureaus of the Department of the Treasury.

In response to your inquiry, Federal law states that the "amount of United States currency notes outstanding and in circulation . . . may not be more than \$300,000,000." 31 U.S.C. § 5115. In current law, however, there is no minimum dollar amount required to be outstanding and in circulation. The law also provides that the Secretary of the Treasury shall "cancel and destroy" any U.S. currency notes presented for redemption. 31 U.S.C. § 5119(b)(2). As part of the CDRI Act, a provision was added that the "Secretary shall not be required to reissue United States currency notes upon redemption." *Id.* It is my understanding that this amendment was added at the request of the Department of the Treasury, which administers and interprets these currency statutes. If you have further

questions regarding this issue or the legislative history of these provisions, you may want to contact the office of the Treasury Under Secretary for Domestic Finance at (202) 622-1703.

If I can be of further assistance, please do not hesitate to contact me.

Sincerely,



Eugene A. Ludwig
Comptroller of the Currency

TESTIMONY OF ROBERT RASOR
DEPUTY ASSISTANT DIRECTOR OF INVESTIGATIONS
UNITED STATES SECRET SERVICE

BEFORE THE HOUSE SUBCOMMITTEE ON DOMESTIC AND INTERNATIONAL
MONETARY POLICY
OF THE
COMMITTEE ON BANKING AND FINANCIAL SERVICES

OCTOBER 11, 1995

MR. CHAIRMAN, THANK YOU FOR THE OPPORTUNITY TO ADDRESS THIS COMMITTEE TODAY ON THE SUBJECT OF THE FUTURE OF MONEY AND THE FUTURE OF PAYMENT SYSTEMS IN THE UNITED STATES AND ABROAD, AND THE PUBLIC POLICY IMPLICATIONS OF THE TECHNOLOGIES INVOLVED. MY NAME IS ROBERT RASOR AND I AM REPRESENTING THE UNITED STATES SECRET SERVICE TODAY IN MY CAPACITY AS THE DEPUTY ASSISTANT DIRECTOR OF INVESTIGATIONS. THAT OFFICE HAS OVERSIGHT RESPONSIBILITY FOR INVESTIGATIONS RELATING TO A VARIETY OF OFFENSES, TO INCLUDE FINANCIAL INSTITUTION FRAUD AND ELECTRONIC CRIMES INVOLVING NETWORK INTRUSIONS, WHERE FUNDS AND DATA ARE STOLEN OR MANIPULATED.

THE SECRET SERVICE IS UNIQUELY QUALIFIED TO DISCUSS WITH YOU TODAY THE PAST, PRESENT, AND FUTURE OF MONEY AND MONETARY TRANSACTIONS IN BOTH A DOMESTIC AND TRANSNATIONAL SENSE. THE JURISDICTION AND RESPONSIBILITY TO DETECT AND INVESTIGATE

FEDERAL INTEREST CRIMES IN THE CREDIT CARD/ACCESS

DEVICE/ELECTRONIC PAYMENT SYSTEMS WAS CONFERRED UPON THE UNITED STATES SECRET SERVICE BY CONGRESS WITH THE PASSING OF THE 1984 COMPREHENSIVE CRIME CONTROL ACT. WE HAVE DEDICATED AN ENTIRE DIVISION AND NUMEROUS FIELD RESOURCES TO COORDINATE THE INVESTIGATION OF CRIMES AGAINST THE FINANCIAL INFRASTRUCTURE, WHICH HAVE INCREASED DRAMATICALLY WITH DEVELOPMENTS IN TECHNOLOGY. THE SPECIFIC STATUTES INCLUDE TITLE 18 USC 1028 (FALSE IDENTIFICATION), 18 USC 1029 (ACCESS DEVICE FRAUD) AND 18 USC 1030 (COMPUTER FRAUD). THE SECRET SERVICE HAS A PROVEN SUCCESS RECORD IN THE INVESTIGATIONS SUPPORTED BY THESE LAWS, INCLUDING BUT NOT LIMITED TO, THE INVESTIGATION OF TELECOMMUNICATION, FINANCIAL INSTITUTION AND ACCESS DEVICE FRAUDS. DURING THE PAST DECADE, THE UNITED STATES SECRET SERVICE HAS DEDICATED COUNTLESS INVESTIGATIVE HOURS TO CONTROL THE COUNTERFEITING AND OTHER FRAUDULENT PAYMENT SCHEMES DEVELOPED TO EXPLOIT THE SYSTEMS. JUST AS IMPORTANT, HOWEVER, IS THE RISK ANALYSIS PROCESS AND THE DEVELOPED UNDERSTANDING THAT THE USSS HAS ACQUIRED IN RELATION TO ELECTRONIC CRIMES AND THE "TECHNO-CRIMINAL."

PROCEEDING WITH A WORKING DEFINITION OF ELECTRONIC CASH AS BEING FINANCIAL COMPENSATION, EXCHANGE OR TRANSFERENCE THROUGH ELECTRONIC MEDIA, THE UNITED STATES SECRET SERVICE HAS AN ESTABLISHED RAPPORT WITH MANY OF THE INDUSTRIES THAT WILL BE CULTIVATING, DEVELOPING AND/OR FACILITATING THIS ACTIVITY. THE TELECOMMUNICATIONS INDUSTRY (WIRELINE AND WIRELESS) IS THE BACKBONE UPON WHICH MUCH OF THIS INDUSTRY IS BEING DEVELOPED. THIS AGENCY HAS WORKED WITH THESE CARRIERS AND MANUFACTURERS FOR YEARS TO IDENTIFY AND ADDRESS VULNERABILITIES INHERENT IN THE DEVELOPMENT OF THEIR RESPECTIVE SYSTEMS AND CLIENTELE. WE HAVE BEEN ASSOCIATED WITH THE CREDIT CARD INDUSTRY AND FINANCIAL INSTITUTIONS AS THEY HAVE EVOLVED THROUGH THEIR MARKETING AND TECHNOLOGICAL EXPANSIONS. WE HAVE WORKED WITH THEM DURING THE DEVELOPMENT OF TELECARDS, SMARTCARDS, BIOMETRIC AUTHENTICATION, AND INTERACTIVE OPPORTUNITIES; AND MOST RECENTLY, AS THEY MANEUVER TO MEET THE DEMANDS FOR ELECTRONIC COMPENSATION. HISTORICALLY, THESE INDUSTRIES AND OUR ECONOMY HAVE BEEN EXPOSED TO MILLIONS OF DOLLARS IN FRAUD AND RELATED EXPLOITATIONS. OUR COMMITMENT HAS CONTRIBUTED TO THE RECOGNITION AND ADOPTION OF POSITIVE SOLUTIONS TO SYSTEMIC PROBLEMS. THE RESULT IS A PRODUCT WHICH IS MORE FRAUD RESISTANT, YET VIABLE IN THE MARKET PLACE.

THROUGH OUR PROACTIVE RISK ANALYSIS PROCESS, WE HAVE COME TO UNDERSTAND THE "SYSTEMS", AND PARTICULARLY THE WEAKNESSES IN THOSE SYSTEMS, THAT ARE OFTEN EXPLOITED BY THE CRIMINAL COMMUNITY. IT IS WITH THIS COLLECTIVE INSTITUTIONAL UNDERSTANDING THAT I WILL TODAY MAKE THE FOLLOWING COMMENTS AND RECOMMENDATIONS.

CIRCA 1865, THE PAYMENT SYSTEM BECAME A NATIONAL CURRENCY, DUE IN PART TO THE FACT THAT ROUGHLY ONE THIRD OF THE CURRENCY IN CIRCULATION IN THE UNITED STATES WAS COUNTERFEIT.

THE UNITED STATES SECRET SERVICE WAS ORIGINALLY CREATED TO COMBAT THE COUNTERFEIT PROBLEM, AN ISSUE WHICH THREATENED THE COUNTRY'S FINANCIAL SYSTEM. TODAY, THE FIGHT AGAINST THE COUNTERFEITING OF U. S. CURRENCY REMAINS A MAJOR PRIORITY OF THE SECRET SERVICE, BOTH DOMESTICALLY AND ABROAD.

IN THE EARLY 1980'S, CREDIT CARDS AND OTHER EMERGING TYPES OF ACCESS DEVICE PAYMENTS WERE TARGETED AND COMPROMISED BY ORGANIZED CRIMINAL ELEMENTS. ALTHOUGH WE CONTINUE TO UTILIZE TECHNOLOGY TO LIMIT THE EFFECTS OF FRAUD, THE CRIMINALS ALSO USE ENHANCED TECHNOLOGY. WE HAVE LEARNED VALUABLE LESSONS IN LAW ENFORCEMENT, AND IN THE VALUE OF LAW ENFORCEMENT ESTABLISHING PARTNERSHIPS WITH BUSINESS

AND INDUSTRY. IN THE EARLY DAYS, CREDIT CARD/ACCESS DEVICE SYSTEMS WERE MARKETING WITH LITTLE REGARD FOR SYSTEM PROTECTIONS, SAFEGUARDS, TRACKING MECHANISMS, AND EVEN SECURITY DEPARTMENTS TO INTERACT WITH LAW ENFORCEMENT WHEN ABUSES WERE DETECTED OR INFORMATION WAS NEEDED. THE LESSON OF THE PAST IS BASIC -- CREATE THE PARTNERSHIPS BEFORE THE SYSTEMS ARE PUT IN PLACE. A GOOD EXAMPLE OF THIS IS THE ELECTRONIC BENEFITS TRANSFER (EBT) TASK FORCE CONCEPT IN WHICH THE GOVERNMENT IS TAKING THE TIME TO APPROPRIATELY DESIGN THE SYSTEM BEFORE IT IS EMPLOYED. CONGRESS MAY ACT AS THE MEDIATOR IN THIS PROCESS BY REQUIRING THE PROPOSED "CYBER" SYSTEMS TO SHOW A DEMONSTRATED ABILITY TO PROTECT THEMSELVES AND ASSIST LAW ENFORCEMENT WHEN DIRECT OR INDIRECT ABUSE OCCURS. A RECOMMENDED APPROACH IS FOR THOSE RESPONSIBLE FOR THE MANAGEMENT AND MARKETING OF THE SYSTEMS TO SPECIFICALLY DEFINE WHAT SERVICES IT PROVIDES. THIS WILL ENABLE LAW ENFORCEMENT TO OUTLINE THE POTENTIAL CRIMINAL ABUSES IN THESE SERVICE AREAS. EXPERIENCE HAS SHOWN THAT PAST, PRESENT AND FUTURE CRIMINAL ACTIVITY IS EVOLUTIONARY IN NATURE AND THE LESSONS LEARNED MAY SERVE TO PREVENT RECURRING AND FUTURE PROBLEMS.

A SECOND RECOMMENDATION FOCUSES ON THE NEED FOR LAW ENFORCEMENT AND THE INDUSTRY TO ESTABLISH AND MAINTAIN ACTIVE WORKING RELATIONSHIPS. FOR THIS EFFORT TO BE PRODUCTIVE, IT MUST BE DELIBERATE AND CONTINUING, RATHER THAN CYCLICAL. THE RELATIONSHIP MUST FACILITATE THE EXCHANGE OF INFORMATION AND TECHNOLOGY. TECHNICAL EVOLUTION HAS NO START UP NOR COMPLETION DATE. BY DEFINITION IT IS ONGOING. EXPERIENCE HAS SHOWN US ALL THAT THE VULNERABILITIES ARE REAL AND OUR PLANNING AND TIMELY RESPONSE ARE ESSENTIAL IN THE AREAS OF POLICY, TECHNOLOGY, AND ENFORCEMENT ISSUES. THE UNITED STATES SECRET SERVICE HAS BEEN DEVELOPING AND MAINTAINING A DIALOGUE WITH THOSE INTERESTED IN THE DEVELOPMENT AND APPLICATION OF CYBER TECHNOLOGY. WE ARE INVOLVED WITH SEVERAL COMMITTEES AND WORKING GROUPS WHICH ARE INTERESTED IN ADDRESSING THESE ISSUES. AS AN EXAMPLE, WE PARTICIPATE IN THE NATIONAL SECURITY INFORMATION EXCHANGE (NSIE) WHICH IS A SUB-GROUP OF THE NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE (NSTAC) WHICH INCLUDES GOVERNMENT AND INDUSTRY REPRESENTATIVES THAT DEAL WITH THREATS, DETERRENTS, VULNERABILITIES, AND PROTECTION MECHANISMS THAT AFFECT THE PUBLIC SWITCH NETWORK. THIS GROUP INCLUDES INTERNET PROVIDERS AND OTHERS THAT ARE PROVIDING OR FACILITATING ELECTRONIC NETWORKS. OTHER SIGNIFICANT GROUPS WITH WHICH WE PARTICIPATE

INCLUDE THE ABA'S LAW ENFORCEMENT AND THE INDUSTRY FOCUS GROUP (LEIFG), THE INTERNATIONAL ASSOCIATION OF CREDIT CARD INVESTIGATORS (IACCI) BOARD OF DIRECTORS, THE DOJ'S NATIONAL TELEMARKETING FRAUD WORKING GROUP, THE FINANCIAL ACTION TASK FORCE, THE NATIONAL PERFORMANCE REVIEW EBT TASK FORCE, AND THE INTERNATIONAL CHIEFS OF POLICE WHICH HAS SEVERAL INITIATIVES TO PREPARE FOR TECHNOLOGICAL ADVANCEMENTS IN CRIMINAL ACTIVITY.

IN CONJUNCTION WITH THESE GROUPS AND OTHERS, THE SECRET SERVICE HAS BEEN ACTIVE IN PREPARING AND UTILIZING RISK ASSESSMENTS TO DETERMINE AND APPRECIATE THE SCOPE OF PROBLEMS WHICH DEVELOP DURING ECONOMIC TRANSITIONS. OUR INPUT WITH THE NSIE RESULTS IN PERIODIC RISK ASSESSMENTS WHICH PROVIDE A PERSPECTIVE ON VULNERABILITIES AND EXPLOITATION OF THE TELECOMMUNICATIONS NETWORK. OUR VARIOUS RISK ASSESSMENTS RELATIVE TO THE CREDIT CARD INDUSTRY IDENTIFIED NUMEROUS PROBLEMS AND CURES OVER THE YEARS WHICH AT TIMES WERE IGNORED BECAUSE THE SYSTEMS WERE TOO ADVANCED AND THE COST TO IMPLEMENT CHANGES WERE PROHIBITIVE. THIS EXPERIENCE ILLUSTRATES THAT NOW IS THE TIME TO ANTICIPATE AND ADDRESS ISSUES IN THIS DEVELOPING AREA. AN EXAMPLE OF RISK ASSESSMENT WHICH ADDRESSES ELECTRONIC COMMERCE ON THE NATIONAL

INFORMATION INFRASTRUCTURE (NII) IS THE SECRET SERVICE REPORT PREPARED IN CONJUNCTION WITH OUR MEMBERSHIP ON THE RISK ASSESSMENT WORKING GROUP OF THE ADMINISTRATION'S INFORMATION INFRASTRUCTURE TASK FORCE, WHICH SPECIFICALLY DESCRIBES THE RISK ASSESSMENT FOR FINANCIAL INSTITUTION USAGE OF THE NII. ALSO, THE SECRET SERVICE WAS A RECENT RECIPIENT OF THE HAMMER AWARD FOR IMPLEMENTING A FINANCIAL CRIMES RISK ANALYSIS MANAGEMENT PROGRAM WHICH ADDRESSES CRIMINAL ACTIVITY DIRECTED TO THE NATION'S FINANCIAL SYSTEM. THE SECRET SERVICE ALSO RECEIVED AN AWARD FROM THE SECRETARY OF THE TREASURY FOR PROACTIVE, INNOVATIVE APPROACHES TO FINANCIAL INSTITUTION FRAUD.

HAVING RECOMMENDED THAT THE CYBER INDUSTRY SHOULD BE HELD ACCOUNTABLE, AND THAT PARTNERSHIPS BE PROMOTED, WE WOULD ALSO PROFFER THAT CONGRESS SHOULD REMAIN ENGAGED IN THIS PROCESS. THE HONORABLE BILL NELSON, CO-SPONSOR OF THE COMPUTER CRIME BILL OF 1984 SAID "WHERE PEOPLE WORK DAILY WITH A POWERFUL TOOL SUCH AS A COMPUTER, THERE WILL BE THOSE WHO OVERSTEP THE BOUNDARIES BETWEEN LEGITIMATE AND CRIMINAL USES OF THESE HIGH-TECHNOLOGY DEVICES." CURRENTLY THE TECHNOLOGY HAS OUTGROWN THE REGULATIONS. THE LAWS WITHIN THIS COUNTRY HAVE TO ADDRESS THESE NEW ISSUES BEFORE WE CAN ASK OTHER

COUNTRIES TO DO AS WE SAY AND NOT AS WE DO. CURRENT INITIATIVES SUCH AS S.982 "NATIONAL INFORMATION INFRASTRUCTURE PROTECTION ACT OF 1995" AND S.1284, "NII COPYRIGHT PROTECTION ACT OF 1995" ENHANCE OUR ABILITY TO INVESTIGATE AND PROSECUTE VIOLATIONS DOMESTICALLY, WHILE OFFERING GUIDELINES FOR FOREIGN GOVERNMENT AUTHORITIES.

CONTINUING INITIATIVES BEING PURSUED BY THE SECRET SERVICE TO PREPARE FOR ELECTRONIC CURRENCY TRANSACTIONS AND OTHER ELECTRONIC COMMERCIAL ENDEAVORS INCLUDES ATTENDING AND SPEAKING AT SEMINARS AND WORKSHOPS ON THE SUBJECT TO INCREASE OUR SHARED KNOWLEDGE AND TO EXPAND OUR LIST OF INDIVIDUAL CONTACTS THAT CAN PROVIDE INSIGHT ON WHERE THE TECHNOLOGY AND MARKETING ARE HEADED. THE SECRET SERVICE IS ALSO IN THE MIDST OF A MAJOR INTERNATIONAL TRAINING INITIATIVE IN EASTERN EUROPE AND SOUTH AMERICA, WHERE WE ARE TRAINING AND INTERACTING WITH BANKS AND LAW ENFORCEMENT WITH THE GLOBAL IMPLICATIONS OF EXCHANGE BEING DISCUSSED AND ANALYZED. KNOWING THE PARTICIPANTS, APPRECIATING THE TECHNOLOGY AND RECOGNIZING APPROPRIATE AREAS FOR INPUT, HAS BEEN THE STRATEGY OF THE SECRET SERVICE IN THE PAST AND CONTINUES WITH THIS LATEST DEVELOPMENT OF ELECTRONIC COMMERCE.

THE EVOLUTION OF THE INTERNET HAS PROVIDED NUMEROUS COMMERCIAL AND FINANCIAL OPPORTUNITIES, SPECIFICALLY IN THE AREAS OF COMMERCE. WITH THE EXPONENTIAL GROWTH OF THE NATIONAL INFORMATION INFRASTRUCTURE THE SAME TYPE OF GROWTH CAN BE EXPECTED IN THE AREAS OF HIGH TECHNOLOGY FRAUD ON A GLOBAL BASIS. DIGITAL CASH MAY WELL BE THE MECHANISM OF THE FUTURE IN WHICH THE MAJORITY OF MONETARY TRANSACTIONS WILL BE CONDUCTED. THIS INCLUDES BOTH ON-LINE AND OFF-LINE EXCHANGES. THE CHALLENGE FACING THE COMMERCIAL, FINANCIAL AND RETAIL ESTABLISHMENTS IS TO DEVELOP THIS TECHNOLOGY ON A RELIABLE, SECURE AND UNIVERSAL PLATFORM. THESE SECURITY FEATURES WILL INCLUDE ENCRYPTION (PUBLIC-KEY, PRIVATE-KEY), DIGITAL SIGNATURE, BIOMETRICS AUTHENTICATION AND THE PHYSICAL SECURITY OF THE MEDIA AND PROCESSING EQUIPMENT. AS RECENT AS THE SEPTEMBER 27TH ISSUE OF THE NEW YORK TIMES THERE IS MENTIONED THE PROPOSAL BY INDUSTRY MEMBERS FOR ESTABLISHING A STANDARD FOR ON-LINE PAYMENT. IT WOULD INCLUDE PUBLIC KEY CRYPTOGRAPHY WHICH WOULD PERMIT TWO PARTIES THAT HAVE NOT PREVIOUSLY EXCHANGED INFORMATION TO CONDUCT A SECRET DATA CONVERSATION. THIS IS BASED ON INDUSTRY TECHNOLOGY WHICH REQUIRES SPECIFIC SOFTWARE THAT WOULD BE DESIGNED TO RUN ON BOTH THE MERCHANT'S AND THE CUSTOMER'S COMPUTER AND PERMIT



THE SECURE AND PRIVATE EXCHANGE OF FINANCIAL INFORMATION. ADDITIONAL INDUSTRY REPRESENTATIVES HAVE BEEN DEVELOPING THEIR OTHER SEPARATE SYSTEMS WHICH PROMOTE INDUSTRY STANDARDS BY MAKING ALL THE SOFTWARE CODE FREELY AVAILABLE TO ANY COMPANY THAT WANTS TO ADOPT IT. IN ADDITION TO THIS NEWSPAPER ARTICLE IS AN OCTOBER 2ND ARTICLE FROM THE WASHINGTON POST'S TECHNOLOGY SECTION WHICH DESCRIBES CONFLICTING VIEWS OF THE INDUSTRY AND THEIR EFFORTS TO AGREE ON BASIC SECURITY STANDARDS TO PROTECT FINANCIAL TRANSACTIONS ON THE INTERNET. THESE ARE TWO EXAMPLES OF HOW TRADITIONAL VENDORS ARE ALIGNING THEMSELVES WITH ELECTRONIC PIONEERS TO MEET THE INEVITABLE DEMAND FOR VIRTUAL TRANSACTIONS. THEIR PROBLEMS OF DEVELOPING, IMPLEMENTING AND DISTRIBUTING AN INDUSTRY STANDARD REFLECTS THE PREDICAMENT BEING FACED BY ALL THE POTENTIAL SERVICE PROVIDERS AS THEY ATTEMPT TO OPEN THIS FRONTIER. THE INDUSTRY ALLIANCES BEING FORMED ARE ALSO SHARP REMINDERS THAT ALTERNATE ELECTRONIC MONEY WILL SOON BE A REALITY GIVEN THE CONSUMER AND INDUSTRY INTEREST IN THE DEVELOPING SERVICES AND BUSINESS OPPORTUNITIES.

THERE CAN BE SAFE ALTERNATIVES TO CURRENCY EXCHANGE ON THE INTERNET AND ALSO OFF-LINE. COMBINING THE LESSONS LEARNED TO

DATE, IMPLEMENTING EXISTING SAFEGUARDS , AND CREATING FUTURE AGREEMENTS IN THE INTERNATIONAL ARENA WILL GUARANTEE THAT SECURE ALTERNATIVES ARE PURSUED. EDUCATION, THE SPREAD OF KNOWLEDGE, AND AN INCREASE IN NECESSARY LAW ENFORCEMENT RESOURCES WILL HELP PROTECT THE UNITED STATES AGAINST INTERNET ATTACKS. THE OBJECTIVE SHOULD BE TO UNDERSTAND AND CONTROL ELECTRONIC MONETARY RISKS AND VULNERABILITIES THUS PROVIDING AND PROMOTING CONFIDENCE TO THIS GLOBAL ELECTRONIC MARKETPLACE OF CONSUMERS, INVESTORS, TAX PAYERS AND THE PUBLIC.

THE UNITED STATES SECRET SERVICE HAS A DECADE OF HANDS ON EXPERIENCE WITH ELECTRONIC CASH AND 125 YEARS OF EXPERIENCE IN CURRENCY PROTECTION. WE STAND READY AND WILLING TO ASSIST IN BUILDING A SAFE, SOUND, AND SECURE MONEY SYSTEM OF THE FUTURE. THERE IS OVERWHELMING EVIDENCE TO INDICATE THAT ECHNOLOGICAL ENHANCED PAYMENT SYSTEMS ARE A REALITY WHICH WILL GROW IN GEOMETRIC PROPORTIONS. IF THE OPPORTUNITY FOR THE INCLUSION OF COMPREHENSIVE SECURITY MEASURES LAPSES, THE DIRECT AND INDIRECT COSTS ASSOCIATED WITH RETROFITTING THE TECHNOLOGY COULD BE DEVASTATING.

THIS CONCLUDES MY REMARKS, MR. HAIRMAN. I WOULD BE HAPPY TO ANSWER ANY OF YOUR QUESTIONS, OR THOSE OF THE COMMITTEE.

ISBN Q-16-052240-4



9 780160 522406